IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

THE TRANSPARENCY PROJECT, Plaintiff, v. U.S. DEPARTMENT OF JUSTICE, et al Defendants.	CIVIL ACTION No. 4:20CV467 JUDGE AMOS MAZZANT

NON-FBI DEFENDANTS' MOTION FOR SUMMARY JUDGMENT

Defendants the United States Department of Justice ("DOJ")[1], the National Security Agency ("NSA"), the Central Intelligence Agency ("CIA"), and the Office of the Director of National Intelligence ("ODNI"), move for summary judgment pursuant to Federal Rule of Civil Procedure 56 and Local Rule 7. The reasons for this motion are set forth in the incorporated briefing, as well as the attached declarations of Vanna Blaine (CIA), Kara Cain (EOUSA), Linda M. Kiyosaki (NSA), Patrick N. Findlay (NSD), Gregory M. Koch (ODNI), and Michael G. Seidel (FBI).

[1] The DOJ components in this case include the National Security Division ("NSD"); the Criminal Division ("CRM"); the Executive Office of United States Attorneys ("EOUSA"); and the Office of Information Policy ("OIP") on behalf of the Offices of the Attorney General ("OAG") and the Office of Legislative Affairs ("OLA").

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Other Authorities

INTRODUCTION

Plaintiff, The Transparency Project, filed this lawsuit pursuant to the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552 *et seq,* based on eight individual requests seeking a wide range of documents submitted to the non-FBI Defendants. In response to Plaintiff's requests, Defendants issued *Glomar* responses to portions of Plaintiff's requests, as appropriate, refusing to confirm or deny the existence or non-existence of certain records, and otherwise produced all responsive records, subject to appropriate withholdings. As set forth in the attached detailed declarations, the non-FBI Defendants have established that the searches were adequate and that the withholdings under each of the FOIA exemptions were proper. This case presents no novel or difficult questions of law. Because Defendants have satisfied their obligations under FOIA, the Court should grant summary judgment in Defendants' favor.

BACKGROUND

I. PLAINTIFF'S FOIA REQUESTS

A. October 26, 2018 Request

On October 26, 2018, Plaintiff submitted a FOIA request to various components of the DOJ, seeking records concerning Imran Awan, Abid Awan, Jamal Awan, Hini Alvi, Rao Abbas, and Seth Rich. Specifically, Plaintiff requested:

1. Documents, files, records, and communications (regardless of electronic, paper or other format) referencing Imran Awan.

2. Documents, files, records, and communications (regardless of electronic, paper or other format) referencing Abid Awan.

3. Documents, files, records, and communications (regardless of electronic, paper or other format) referencing Jamal Awan.

4. Documents, files, records, and communications (regardless of electronic, paper or other format) referencing Hina Alvi.

5. Documents, files, records, and communications (regardless of electronic, paper or other format) referencing Rao Abbas.

6. From the National Security Division only, I request documents, files, records, and communications (regardless of electronic, paper or other format) referencing Seth Conrad Rich or "Seth Rich," who is deceased.

[ECF No. 5, Exh. 1].

B. October 29, 2018 Request

On October 29, 2018, Plaintiff submitted a FOIA request to the NSA seeking communications with members of Congress regarding various individuals. Specifically, Plaintiff requested:

1. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Seth Conrad Rich.

2. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Julian Assange.

3. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Wikileaks.

4. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Kim Dotcom.

5. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee)

since January 1, 2016 regarding or referencing Aaron Rich.

6. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Shawn Lucas.

7. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Kelsey Mulka.

8. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Imran Iwan.

9. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Abid Awan.

10. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Jamal Awan.

11. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Hina Alvi.

12. All correspondence received from or sent to any member of Congress (or anyone representing a member of Congress or Congressional committee) since January 1, 2016 regarding or referencing Rao Abbas.

[ECF No. 5, Exh. 2].

A. May 28, 2020 Request

On May 28, 2020, Plaintiff submitted a FOIA request to the CIA seeking various records. Specifically, Plaintiff requested:

1. I request the opportunity to view all metadata, communications (internal or external), records, documents, reports or other evidence regarding whether the CIA, its Directorate of Digital Innovation, or any of the CIA's foreign or domesticaffiliates, agents, employees or contractors played a

role in inserting Russian"fingerprints" (*e.g.*, "COZY BEAR" or "FANCY BEAR") into data from the 2016Data Breach. In other words, the CIA should produce all evidence indicating whether the CIA, its Directorate of Digital Innovation or any of the CIA's foreign or domestic affiliates, agents, employees or contractors inserted or fabricatedevidence to make it appear that Russians or other third parties were responsible forthe 2016 Data Breach. This includes, for example, any and all evidence that the Directorate of Digital Innovation created or operated the "Guccifer 2.0" or "DCLeaks" profiles or any other online profile used to promote or distribute data from the 2016 Data Breach.

2. I request the opportunity to view all tangible evidence indicating whether the 2016 Data Breach was the result of (1) outside forces (*e.g.*, Russian agents,Pakistani agents, etc.) who hacked the servers from a remote location or (2) an individual or individuals who were present at or inside DNC facilities and copied the data onto a storage device. If, for example, the CIA obtained any communications between Seth Rich and Julian Assange or Wikileaks (*e.g.*, from the National Security Agency, the United Kingdom's Government Communications Headquarters, or any other person or entity), then those communications should be produced. If the CIA has any evidence whatsoever that the DNC servers were hacked externally or that DNC data was leaked from an internal source, that evidence should be produced.

3. Former CIA Director John Brennan testified that in the summer of 2016, he convened a task force / working group involving the CIA, NSA and FBI toinvestigate intelligence showing contact between Russian officials and Trump affiliates. I wish to view all documents, records, and/or communications that (1) identify the name and agency affiliation of each member of the task force /working group as well as (2) the dates that each such person began and ceased working with the group. I also wish to view all documents, records, and/orcommunications indicating whether the task force / working group fabricated or attempted to fabricate evidence of collusion between Donald Trump (or his presidential campaign) and Russian officials. If, for example, individuals from thetask force tried to create the false impression that Trump campaign officials were acting at the behest of Russian officials, any and all evidence of that should be produced.

4. For the period from January 20, 2009 until the present, I wish to see all documents, records, communications, and guidelines reflecting any plans

or efforts by the CIA to gain, cultivate or exercise influence over any U.S. journalist or journalism entity. This request includes, but is not limited to, documents or communications that reflect an attempt to insert CIA personnel, contractors, or allies into U.S. media companies. This request further includes, but is not limited to, documents reflecting payments (direct or indirect) to U.S. journalists or journalism entities.

5. For the period from January 20, 2009 until the present, I wish to see all documents, records, communications, and guidelines reflecting any plans or efforts by the CIA to gain, cultivate or exercise influence over any U.S. social media company (*e.g.*, Facebook or Twitter) for purposes of influencing its algorithms or the prevalence of (1) particular posts or publications or (2) particulartypes of posts or publications. This request includes, but is not limited to, documents or communications that reflect an attempt to insert CIA personnel, contractors, or allies into such a company.

6. For the period from January 20, 2009 until the present, I wish to see all documents, records, communications, and guidelines reflecting any plans or efforts by the CIA to gain, cultivate or exercise influence over any U.S. search engine company (*e.g.*, Google) for purposes of influencing its algorithms or the prevalence of search results. This request includes, but is not limited to, documents or communications that reflect an attempt to insert CIA personnel, contractors, or allies into such a company.

7. For the period from January 20, 2009 until the present, I wish to see all documents, records, communications, and guidelines reflecting any plans or efforts by the CIA to surveil journalists and/or journalism companies in the UnitedStates. This request includes, but is not limited to, (1) plans or efforts to hack into the computer systems, online accounts, or electronic devices of journalists orjournalism companies in the United States, and (2) any documents, records, or communications obtained as a result of such hacking efforts. This request further includes, but is not limited to, documents, records, or communications identifying (1) the CIA affiliates, agents, employees or contractors involved in such activities,and (2) the targets of any such activities.

8. For the period from January 20, 2009 until the present, I wish to see all documents, records, communications, and guidelines reflecting any plans or efforts by the CIA to influence the contents of any entertainment

production in theUnited States, *e.g.*, movies, television programs, radio programs, podcasts, Netflix productions, etc.

[ECF No. 5, Exh. 3].

B. June 5, 2020 Request

On June 5, 2020, May 28, 2020, Plaintiff submitted a FOIA request to the ODNI seeking various records. Specifically, Plaintiff requested:

1. I request the opportunity to view all tangible evidence indicating whether the 2016 Data Breach was the result of (1) outside forces (*e.g.*, Russian agents, Pakistani agents, etc.) who hacked the servers from a remote location or (2) an individual or individuals who were present at or inside DNC facilities and copied the data onto a storage device. If, for example, ODNI possesses any communications between Seth Rich and Julian Assange or Wikileaks (*e.g.*, from the National Security Agency, the United Kingdom's Government Communications Headquarters, or any other person or entity), then those communications should be produced. If the ODNI has any evidence whatsoever that the DNC servers were hacked externally or that DNC data was leaked from aninternal source, that evidence should be produced.

2. Former CIA Director John Brennan testified that in the summer of 2016, he convened a task force / working group involving the CIA, NSA and FBI to investigate intelligence showing contact between Russian officials and Trumpaffiliates. I wish to view all documents, records, and/or communications that (1) identify the name and agency affiliation of each member of the task force /working group as well as (2) the dates that each such person began and ceased working with the group. I also wish to view all documents, records, and/orcommunications indicating whether the task force / working group fabricated or attempted to fabricate evidence of collusion between Donald Trump (or his presidential campaign) and Russian officials. If, for example, individuals from thetask force tried to create the false impression that Trump campaign officials were acting at the behest of Russian officials, any and all evidence of that should be produced.

3. All data, documents, records, or communications (electronic or otherwise) created, received or obtained since January 1, 2016 that discuss or reference Seth Conrad Rich ("Seth Rich") or Aaron Nathan Rich ("Aaron Rich").

4. All data, documents, records, or communications regarding any person or entity's attempt to hack into Seth Rich's electronic or internet accounts (*e.g.*, email) after his death.

5. All data downloaded from all electronic devices that belonged to Seth Rich as well as all data, documents, records or communications indicating how the devices were obtained and who was responsible for downloading the information.

6. All data, documents, communications, records or other evidence indicating whether Seth Rich, Aaron Rich, or any other person or persons were involved in transferring data from the Democratic National Committee to Wikileaks in 2016, either directly or through intermediaries. This request includes, but is not limited to, any reports from CrowdStrike, Inc.

7. All documents, records, or communications exchanged with Congress or any other government agencies (or representatives of such agencies) since January 1, 2016 regarding (1) Seth Rich's murder or (2) Seth Rich's or Aaron Rich's involvement in transferring data from the Democratic National Committee to Wikileaks.

[ECF No.5, Exhibit 4].

C. June 11, 2020 Request

On June 11, 2020, Plaintiff submitted a FOIA request to various components of the DOJ seeking records related to investigations of former congressional IT support staffers. Specifically, Plaintiff requested:

1. Any and all records related to any investigations or preliminary investigations involving former congressional IT support staffers Abid Awan, Imran Awan, Jamal A wan, and Hina R. Alvi. As part of this request, searches should of records[sic] should include, but not be limited to, the FBI automated indices, its older manual indices, and its Electronic Surveillance (EL SUR) Data Management System (EDMS), as well as cross-referenced files.

2. Any and all records of communication sent to or from FBI employees, officialsor contractors involving the subjects in [the item above].

[ECF No. 5, Exhibit 6].

D. June 12, 2020 Request

On June 12, 2020, Plaintiff submitted a FOIA request to the NSA seeking records related to the 2016 Data Breach. Specifically, Plaintiff requested:

1. I request the opportunity to view all metadata, communications (internal or external), records, documents, reports or other evidence regarding whether the National Security Agency ("NSA"), the Central Intelligence Agency ("CIA"), any "Five Eyes" allies, and/or affiliates, agents, employees or contractors of those agencies or any other government entity played a role in inserting Russian "fingerprints" (*e.g.*, "COZY BEAR" or "FANCY BEAR") into data from the 2016Data Breach. In other words, the NSA should produce all evidence indicating whether any U.S. Government or "Five Eyes" entities, affiliates, agents, employees or contractors inserted or fabricated evidence to make it appear that Russians or other third parties were responsible for the 2016 Data Breach. This includes, for example, any and all evidence that U.S. Government or "Five Eyes" entity, affiliate, agent, employee, or contractor created or operated the "Guccifer 2.0" or "DCLeaks" profiles or any other online profile used to promote or distribute data from the 2016 Data Breach.

2. I request the opportunity to view all tangible evidence reflecting the person, persons, or entities involved in 2016 Data Breach. This request includes, but is notlimited to, evidence indicating whether the breach was the result of (1) outside forces (*e.g.*, Russian agents, Pakistani agents, etc.) who hacked the servers from a remote location or (2) an individual or individuals who were present at or inside DNC facilities and copied the data onto a storage device. If, for example, NSA intercepted or obtained any communications between Seth Rich and Julian Assange or Wikileaks (*e.g.*, from the United Kingdom's Government Communications Headquarters, or any other person or entity), then those communications should be produced. If the NSA has any evidence whatsoever that the DNC servers were hacked externally or that DNC data was leaked from an internal source, that evidence should be produced.

3. I request the opportunity to view all communications exchanged (either directly orindirectly) between Seth Conrad Rich ("Seth Rich") and/or

> Aaron Nathan Rich ("Aaron Rich") and the following: Julian Assange, Wikileaks, and/or any agentsor representatives of Wikileaks.

[ECF No. 5, Exhibit 7].

E. June 15, 2020 Request

On June 15, 2020, Plaintiff submitted a FOIA request to the NSD seeking records about the DNC email hack. Specifically, Plaintiff requested:

1. All documents, records, communications, and other tangible evidencesupporting Gen. Demers's claims to *60 minutes* above, *i.e.*, about Russian involvement in obtaining the DNC emails in 2016.

2. All documents, records, communications, and other tangible evidence relied onby Gen. Demers, Adam Hickey, Sean Newell, and Heather Alpino in support of their conclusions that Russians were responsible for obtaining the DNC emails in 2016.

3. All documents, records, communications, and other tangible evidence in the possession or control of the National Security Division concerning Seth Conrad Rich and/or Aaron Nathan Rich.

4. All documents, records, communications, and other tangible evidence in the possession or control of the National Security Division concerning other entities or individuals who may have played a role in stealing, hacking, leaking or improperly obtaining the DNC emails in 2016.

5. All documents, records, communications, and other tangible evidence in the possession or control of the National Security Division indicating whether the DNC emails were hacked externally, leaked from a source inside the DNC, or otherwise transmitted to third parties such as Wikileaks. If there was one or more than one instance of hacking, leaking, or other unauthorized transmission of DNC emails in 2016, please provide details for each such incident, *e.g.*, the dates, persons and entities involved, the data that was hacked, leaked, or otherwise transmitted, and the means by which it was hacked, leaked, or transmitted.

6. All documents, records, communications, and other tangible evidence in the possession or control of the National Security Division or the FBI regarding whether Debbie Wasserman-Shultz or any other member of Congress was

blackmailed or extorted, whether directly or indirectly, as a result of information procured by any of the following: Imran Awan, Abid Awan, Jamal Awan, Hina Alvi, Rao Abbas, or anyone affiliated with the government of Pakistan.

[ECF No. 5, Exhibit 8].

F. June 18, 2020 Request

On June 18, 2020, Plaintiff submitted a FOIA request to CIA, DOJ, and NSA seeking records related to surveillance of Edward Butowsky or Matt Couch, as well as CIA Director David Petraeus. Specifically, Plaintiff requested:

1. I request the opportunity to view all documents, records, communications and/or other tangible evidence reflecting or pertaining to surveillance of Edward Butowsky of Texas or Matt Couch of Arkansas. The term "surveillance" includes, but is not limited to, any attempt to hack into the computers, phones, otherelectronic devices, and/or online accounts of Mr. Butowsky or Mr. Couch. If any information obtained by surveillance was relayed to third parties, that information should be produced for inspection.
2. I request the opportunity to view all documents, records, communications and/or other tangible evidence pertaining to whether former Central Intelligence Agency Director David Petraeus mishandled classified information or sold such information during his tenure as CIA director. This request includes, but is not limited to, documents, records, communications and/or other tangible evidence in the possession of the Office of the Inspector General of the CIA and/or the Office of the Intelligence Community Inspector General. This request further includes, but is not limited to, any draft indictments, draft arrest warrants, actual arrest warrants, and/or records of arrest.

[ECF No. 5, Exhibit 9].

II. PROCEDURAL HISTORY BY AGENCY

A. EOUSA (October 26, 2018 & June 11, 2020 Requests)

On October 26, 2018, Plaintiff submitted a FOIA request to EOUSA. [ECF No. 5, Exhibit 1]. EOUSA acknowledged receipt of the request and assigned it request number EOUSA-2019-000496. [Cain Declaration, Exhibit B].

Plaintiff did not provide authorization of release from any of the individuals outlined in the request. Absent certification which would authorize release of third-party information, EOUSA directed the United States Attorney's Office for the District of Columbia ("USAO-DC") to conduct a search for public records responsive to plaintiff's request on November 2, 2018. [Cain Declaration].

EOUSA Policy dictates that if a requester obtains the written authorization and consent of the third parties for release of records, the requester may submit a new request for the documents accompanied with the written authorization. EOUSA never received such authorization. [Cain Declaration].

EOUSA submitted a second search request for EOUSA-2019-000496 to USAO-DC on August 14, 2020. On April 16, 2021, USAO-DC provided EOUSA FOIA/PA Office with public records responsive to the request. [Cain Declaration].

EOUSA provided its final response for EOUSA-2019-000496 on June 25, 2021. The final disposition consisted of eight pages released in full and ten pages released in part. [Cain Declaration, Exhibit C].

EOUSA was made aware of a second FOIA request dated June 11, 2020, via this litigation. The request was submitted as a follow-up request. EOUSA assigned the request number EOUSA-2020-004715. The request sought the records that the Federal Bureau of Investigation ("FBI") provided to Judicial Watch in *Judicial Watch v. Department of Justice* 1:18-cv-02563. [Cain Declaration].

Since any records provided in response to *Judicial Watch v. Department of Justice* would have been released by FBI, it was determined that the request was under the purview of the FBI. A *Misdirected Request Letter* was submitted to the requester on January 12, 2021, and the request was subsequently closed. [Cain Declaration, Exhibit D]. Plaintiff has indicated that he is not challenging EOUSA's disposition of the June 11, 2020, request.

B. NSD (October 26, 2018, June 11, 2020, June 15, 2020 & June 18, 2020 Requests)

Related to this litigation, NSD received four FOIA request from Plaintiff by electronic filing. The first was dated October 26, 2018. [ECF No. 5, Exhibit 1]. The second was dated June 11, 2020. [ECF No. 5, Exhibit 6]. The third was dated June 15, 2020. [ECF No. 5, Exhibit 8]. The fourth was dated June 18, 2020. [ECF No. 5, Exhibit 9]. The FOIA requests dated October 26, 2018, and June 15, 2020, sought the same records. [Findlay Declaration].

On September 2, 2020, NSD responded to the June 11, 2020, request noting that the request was assigned tracking number NSD 20-341. [Findlay Declaration, Exhibit E]. In that same email, NSD further informed Plaintiff that it does not maintain FBI records

and sought clarification. NSD went on to note that, as such, if NSD did not receive a response within 30 days, the request would be administratively closed. NSD did not receive such a response, and NSD 20-341 was administratively closed accordingly. [Findlay Declaration].

On November 5, 2020, NSD responded to the June 15, 2020, request noting that the was request was assigned tracking number NSD 20-333. [Findlay Declaration, Exhibit F]. NSD issued an interim response to NSD 20-333 on March 9, 2021. [Findlay Declaration, Exhibit G]. In this response, NSD FOIA released one 40-page record in part, with redactions made pursuant to FOIA Exemption 6. [Findlay Declaration]. NSD issued a final response to NSD 20-333 on August 30, 2021, whereby it released one record that was 149 pages in length. The only redactions were done pursuant to FOIA Exemption 6. [Findlay Declaration, Exhibits H & I].

On November 16, 2021, NSD issued a final response to the request dated June 18, 2020, noting that the request was assigned tracking number NSD 20-338. NSD declined to confirm or deny the existence of records responsive to part one of this request, a so-called *Glomar* response, pursuant to FOIA Exemption 1. In addition, NSD released one record in full as responsive to part two of this request. Finally, NSD noted that it had referred one additional record to a different component of the Department for direct response to Plaintiff. [Findlay Declaration, Exhibits J & K].

C. NSA (October 29, 2018 & June 12, 2020 Requests)

On October 29, 2018, Plaintiff submitted a FOIA request to NSA. [ECF No. 5, Exhibit 2]. In response, NSA sent a letter on October 31, 2018, informing Plaintiff that the request was assigned Case Number 105508. NSA conducted a search for responsive records and by letter dated February 2, 2021, provided five records, totaling 13 pages, to Plaintiff. NSA also explained that six records, which totaled 16 pages, were being withheld in their entirety pursuant to FOIA Exemptions 1, 3, 5, and 6. First, the letter explained that because the information was currently and properly classified in accordance with E.O. 13526, it was exempt from disclosure based on Exemption 1. Second, the letter explained that the same information was also protected from release by statute, and thus also exempt from release based upon Exemption 3. Specifically, the letter cited three statutes applicable to the case: 18 U.S.C. § 798, 50 U.S.C. § 30240), and Section 6 of Public Law 86-36 (codified at 50 U.S.C. § 3605). Third, the letter stated that the information was being withheld under Exemption 5 because the information was protected by deliberative process privilege.[2] Finally, the letter explained that individuals' personal information was being withheld under Exemption 6 because the individuals' privacy interests outweighed the public interest for the information. [Kiyosaki Declaration, Exhibit B].

[2] Although NSA asserted Exemption 5 in the response letter, after further review, NSA determined that Exemption 5 was inappropriate. Nonetheless, much of the information was properly redacted under Exemptions 1 and 3 pursuant to Section 6 of the National Security Agency Act of 1959 (Pub. L. No. 86-36, codified at 50 U.S.C. § 3605). NSA has prepared a reissuance of the documents with the proper redactions cited, contained in Exhibit F to the Kiyosaki Declaration.

On June 12, 2020, Plaintiff submitted a FOIA request to NSA. [ECF No. 5, Exhibit 7]. In response, NSA sent a letter on June 19, 2020, informing Plaintiff that the request was assigned Case Number 109745. [Kiyosaki Declaration, Exhibit C]. On January 20, 2021, NSA issued a *Glomar* response based on Exemptions 1 and 3 of the FOIA. [Kiyosaki Declaration, Exhibit C]. On February 1 1, 2021, Plaintiff appealed NSA's Glomar response. [Kiyosaki Declaration, Exhibit D].

D. CIA (May 28, 2020 & June 18, 2020 Requests

On May 28, 2020, Plaintiff submitted a FOIA request to the CIA. [ECF No. 5, Exhibit 3]. The CIA acknowledged receipt of the request via letter dated June 15, 2020. [Blaine Declaration, Exhibit C].

On June 18, 2020, Plaintiff submitted a second FOIA request to the CIA. [ECF No. 5, Exhibit 9]. On June 4, 2021, the CIA sent Plaintiff an interim response letter to the two CIA requests. [Blaine Declaration, Exhibit E]. The interim response letter was returned to the CIA as unclaimed. [Blaine Declaration, Exhibit F].

On July 13, 2021, the CIA sent Plaintiff a final response to the two CIA requests. [Blaine Declaration, Exhibit G]. The CIA withheld six documents in full in response to parts 3(1) and 3(2) of the May 2020 CIA Request. The CIA cited Exemptions 1, 3, 5, and 6 as the basis for the withholdings. [Id.].

The CIA also released in part four documents and withheld in full 157 documents responsive to part 2 of the June 2020 CIA Request. The CIA cited Exemptions 1, 3, 5, 6,

and 7(C) & (E) as the basis for the withholdings. [Blaine Declaration, Exhibit G]. The CIA's Final Response Letter should have also cited Exemption 7. [Blaine Declaration].

As to the remainder of the CIA requests, the CIA issued a *Glomar* response in response to Parts 1, 2, 3(3), 4, 5, 6, 7, and 8 of the May 2020 CIA Request, and Part 1 of the June 2020 CIA Request. [Blaine Declaration, Exhibit G].

E. ODNI (June 11, 2020 Request)

On June 11, 2020, Plaintiff submitted a FOIA request to ODNI. [ECF No. 5, Exhibit 6]. By letter dated July 6, 2020, ODNI acknowledged receipt of the request and assigned it tracking number DF-2020-00296. [Koch Declaration, Exhibit B].

By letter dated September 1, 2021, ODNI provided Plaintiff with its final response, indicating that nineteen documents were withheld in full, four documents were withheld in part, and three documents were referred to other agencies. The letter also explained that other agencies reviewed their equities within the documents and listed the exemptions claimed by those agencies. [Koch Declaration, Exhibit C].

F. OIP on behalf of OLA/OAG (October 26, 2018 & June 11, 2020 Requests)

Plaintiff has indicated that he is not challenging OIP's searches and "no records" responses in both requests.

G. CRM (October 26, 2018 & June 11, 2020 Requests)

As to the October 26, 2018, request, Plaintiff has conceded exhaustion. [ECF No. 28]. As to the June 11, 2020, request, Plaintiff has indicated that he is not challenging CRM's search and "no records" response to this request.

LEGAL STANDARDS

Summary judgment is appropriate when there is no genuine issue as to any material fact and the moving party is entitled to judgment as a matter of law. *See* Fed. R. Civ. P. 56(a); *Diamond v. Atwood*, 43 F.3d 1538, 1540 (D.C. Cir. 1995). FOIA actions are typically resolved on summary judgment, *see Reliant Energy Power Generation, Inc. v. FERC*, 520 F. Supp. 2d 194, 200 (D.D.C. 2007), and the Court conducts a *de novo* review of the agency's response to any challenged FOIArequests, *see* 5 U.S.C. § 552 (a)(4)(B). When a requester challenges the adequacy of an agency's search, "[i]n order to obtain summary judgment, the agency must show that it made a good faith effort to conduct a search for the requested records, using methods which can be reasonably expected to produce the information requested." *Oglesby v. U.S. Dep't of the Army*, 920 F.2d 57,68 (D.C. Cir. 1990); *see Weisberg v. U.S. Dep't of Justice*, 745 F.2d 1476, 1485 (D.C. Cir. 1984).The agency must also justify any records withheld (in whole or in part) subject to FOIA's statutory exemptions. Congress recognized "that legitimate governmental and private interests could be harmed by release of certain types of information and provided nine specific exemptions under which disclosure could be refused." *FBI v. Abramson*, 456 U.S. 615, 621 (1982). "Summary judgment is warranted on the basis of agency affidavits when the affidavits describe the justifications for nondisclosure with reasonably specific detail, demonstrate that the information withheld logically falls within the claimed exemption, and are not controverted by either contrary evidence in the record nor by evidence of agency bad faith." *Larson v. U.S. Dep't of State*, 565F.3d

857, 865 (D.C. Cir. 2009) (quotation omitted). "Ultimately, an agency's justification for invoking a FOIA exemption is sufficient if it appears 'logical' or 'plausible.'" *Wolf v. CIA*, 473F.3d 370, 374-75 (D.C. Cir. 2007) (citing *Gardels v. CIA*, 689 F.2d 1100, 1105 (D.C. Cir. 1982); *Hayden v. NSA*, 608 F.2d 1381, 1388 (D.C. Cir. 1979)).

STATEMENT OF THE ISSUES

1. Whether Defendants conducted reasonable searches in response to Plaintiff's FOIA requests;

2. Whether Defendants properly issued *Glomar* responses in partial response to Plaintiff's FOIA requests; and

3. Whether Defendants properly withheld information pursuant to FOIA exemptions in response to Plaintiff's FOIA requests.

ARGUMENT & AUTHORITIES

I. DEFENDANTS CONDUCTED REASONABLE SEARCHES

Courts require agencies to conduct searches "reasonably calculated to uncover all relevant documents." *Campbell v.* SSA, 446 F.App'x 477, 480 (3rd Cir. June 3, 2011)(quoting *Weisberg v.* DOJ, 705 F.2d 1344, 1351 (D.C. Cir. 1983)). The Court may grant summary judgment concerning the adequacy of an agency's search for responsive records based on information provided in "[a] reasonably detailed affidavit, setting forth the search terms and the type of search performed, and averring that all files likely to contain responsive materials (if such records exist) were searched." *Valencia–Lucena v. U.S. Coast Guard*, 180 F.3d 321, 326 (D.C. Cir. 1999) (quoting *Oglesby*, 920 F.2d at 68); *see Meeropol v. Meese*, 790 F.2d 942, 952-53 (D.C. Cir. 1986). "Such agency

affidavits attesting to a reasonable search 'are afforded a presumption of good faith,' and 'can be rebutted only with evidence that the agency's search was not made in good faith.'" *Defenders of Wildlife v. U.S. Dep't of Justice*, 314 F. Supp. 2d 1, 8 (D.D.C. 2004) (quoting *TransUnion, LLC v. FTC*, 141 F. Supp. 2d 62, 64 (D.D.C. 2001)).

"Adequacy - not perfection - is the standard that FOIA sets," and agencies "need not knock down every search design advanced by every requester." *DiBacco v. U.S. Army*, 795 F.3d 178, 191 (D.C. Cir. 2015). Conducting a "reasonable" search is a process that requires "both systemic and case-specific exercises of discretion and administrative judgment and expertise" and is "hardly an area in which the courts should attempt to micro manage the executive branch." *Schrecker v. U.S. Dep't of Justice*, 349 F.3d 657, 662 (D.C. Cir. 2003) (quotation omitted).

To that end, in evaluating the adequacy of a search, courts accord agency affidavits a presumption of good faith that cannot be rebutted by speculation "about the existence and discoverability of other documents." *SafeCard Servs., Inc. v. SEC*, 926 F.2d 1197, 1200 (D.C. Cir.1991) (internal quotation and citation omitted); *see also Ground Saucer Watch, Inc. v. CIA*, 692 F.2d 770, 771 (D.C. Cir. 1981) (same). Rather, to establish the sufficiency of its search, the agency's affidavits need only explain the "scope and method of the search" in "reasonable detail."*Kidd v. U.S. Dep't of Justice*, 362 F. Supp. 2d 291, 295 (D.D.C. 2005); *see also*, *Hefferman v. Azar*, 417 F.Supp. 3d 1, 12 (explaining that agency "properly searched the files of all potential custodians who reasonably could have possessed [records]" where agency identified the

specific custodians and locations searched and also confirmed why others were not searched.). FOIA does not require agencies to search every record system, but only those systems in which the agency believes responsive records are likely to be located. *W. Ctr. for Journalism v. IRS*, 116 F. Supp. 2d 1, 9 (D.D.C. 2000), *aff'd*, 22 F. App'x 14 (D.C. Cir. 2001); *Roberts v. U.S. Dep't of Justice*, Civ. A. No. 92-1707 (NHJ), 1995 WL 356320, at *1 (D.D.C. Jan. 29, 1993). As explained below, a reasonable search is precisely what Defendants performed here.

A. EOUSA's Search for Responsive Records

The details of EOUSA's search are set forth in the Declaration of Kara Cain on pages 4-5, paragraphs 13-19. Only the October 26, 2018, request seeking records regarding Imran Awan, Abid Awan, Jamal Awan, Hina Alvi, Rao Abbas, and Seth Rich is at issue for EOUSA, as set forth in the procedural history above. Specifically, Ms. Cain explains that any records pertaining to a criminal investigation involving these individuals would be maintained in the U.S. Attorney's Office ("USAO") where the prosecutions took place, in this case the USAO-DC. [Cain Declaration, ¶14].

Ms. Cain explains that cases are opened, updated, and saved under the name of the defendant. Any associated records or matters would be located upon a search of a defendant's name. Any co-defendants would be added under the case management feature of the database. In the electronic case folder, each co-defendant would have their own sub-folder with associated records. [Cain Declaration, ¶15].

The USAO-DC FOIA contact organized a search for records responsive to

Plaintiff's FOIA request. The search was initiated by reviewing the online case management system using the names and subject matter provided in the original request. The online tracking system utilized by the USAOs is CaseView. The CaseView database is used to track cases and retrieve files related to cases and investigations by using district court case numbers, defendants' name, and the internal number assigned by each USAO. After a search of CaseView, on April 16, 2021, USAO-DC provided EOUSA FOIA/PA Office with unsealed, public records responsive to the request. [Cain Declaration, ¶16-19].

B. NSA's Search for Responsive Records

The details of NSA's search are set forth in Section IV, Paragraphs 15-21, pages 10-11 of the Declaration of Linda M. Kiyosaki. The Agency tasked its Legislative, State, Local, and Academic Engagement office ("LSLA") to search its records. Personnel from NSA's Office of General Counsel ("OGC"), in coordination with the FOIA Office, directed and assisted in the search for responsive records. NSA OGC, in coordination with the FOIA Office, determined that LSLA was the most likely NSA organization to possess responsive records, to the extent responsive records existed, and that no other components of NSA were reasonably likely to possess additional materials responsive to Plaintiff's request. [Kiyosaki Declaration, ¶15].

In tasking this search, NSA OGC directed LSLA to search the office's records in all places where records responsive to the October 2018 FOIA request were most likely to be found. NSA OGC recommended that LSLA search its records for "[e]ach of the 12

names as written" and "[v]ariations on each of the 12 names including: last name only; first and last name; and first, middle (if known), and last name." [Kiyosaki Declaration, ¶16].

After collecting potentially responsive records from LSLA, personnel from OGC conducted a first-level review of the materials to determine if they were, in fact, responsive to Plaintiff's request. OGC personnel then conducted a second-level review of selected materials to determine, in certain instances, responsiveness, as well as segregability. Ultimately, OGC determined that there were eleven records responsive to Plaintiff's October 2018 FOIA request. [Kiyosaki Declaration, ¶17].

OGC determined that five responsive documents were segregable, containing non-exempt material releasable to Plaintiff. In coordination with the FOIA Office, NSA redacted certain information from these documents, which is exempt from disclosure, as detailed below. [Kiyosaki Declaration, ¶18].

OGC also determined that six documents contained exempt material and were non-segregable. Therefore, NSA withheld those documents from Plaintiff in full for the reasons explained below. [Kiyosaki Declaration, ¶19].

NSA identified and searched the NSA components that were likely to possess records responsive to the FOIA request and identified and used search methods that were reasonably likely to identify all responsive NSA records. This approach resulted in the release of five documents to Plaintiff that were determined to contain segregable non-exempt information. Additional pages of responsive material were identified during the

course of this search and were determined by OGC personnel to contain non-segregable information that is both classified and protected from disclosure by statute. [Kiyosaki Declaration, ¶21].

C. CIA's Search for Responsive Records

The details of CIA's search are set forth in Section IV, paragraphs 30-33, pages 16-18 of the Declaration of Vanna Blaine. The CIA processed documents in responses to parts 3(1) and 3(2) of the May 2020 CIA Request. These requests relate to the task force/working group convened by former CIA Director John Brennan. In particular, parts 3(1) and 3(2) seek records that the CIA "(1) identify the name and agency affiliation of each member of the task force/working group as well as (2) the dates that each such person began and ceased working with the group." The CIA also processed documents in response to part 2 of the June 2020 CIA Request, which requested records "pertaining to whether former Central Intelligence Agency Director David Petraeus mishandled classified information or sold such information during his tenure as CIA director." [Blaine Declaration, ¶30].

In response to these parts of the requests, CIA conducted broad searches designed to uncover any responsive documents located across the Agency. The CIA first identified the offices that were most likely to maintain responsive materials. These were the Office of the Director, the Office of Congressional Affairs, the Office of the Inspector General (OIG), the Office of General Counsel, and the Office of Security. [Blaine Declaration, ¶31].

Agency professionals conducted searches spanning the pertinent time frame appropriate for each of these two requests. These searches included emails, internal share drives, relevant databases, and paper files. Additionally, search personnel also queried CADRE, the Agency's repository for records that have been previously disclosed to the public. [Blaine Declaration, ¶32].

As a result of these searches, the CIA identified six records responsive to parts 3(1) and 3(2) of the May 2020 CIA Request. The CIA withheld all six of these records in their entirety. In addition, the CIA identified 161 records responsive to part 2 of the June 2020 CIA Request. Of this number, the CIA withheld 157 records in their entirety, and released four in part. [Blaine Declaration, ¶33].

D. ODNI's Search for Responsive Records

The details of ODNI's search are set forth in Section V, paragraphs 16-17, pages 6-7 of the Declaration of Gregory M. Koch. Given the subject matter of the Plaintiff's Request, and in accordance with standard processing protocols, ODNI's Information Management Office ("IMO") tasked two ODNI components—Mission Integration and the National Counterintelligence and Security Center—to search for potentially responsive records. Those components were chosen because they are the components most likely to have information responsive to the Request. [Koch Declaration, ¶16].

Because the documents that ODNI identified as being responsive to Plaintiff's Request included information from other IC elements, ODNI engaged in consultations with the Department of Homeland Security, the Defense Intelligence Agency, U.S.

European Command, the Federal Bureau of Investigation, the Naval Criminal Investigative Service, and the Department of State. Through that consultation process, the other agencies identified their equities in the responsive ODNI documents, and ODNI applied relevant and appropriate FOIA exemptions on behalf of those agencies. [Blaine Declaration, ¶17].

E. Defendants' Searches Were Adequate

The declarations submitted along with this motion demonstrate that the non-FBI Defendants "made a good faith effort to conduct…search[es] for the requested records, using methods which can be reasonably expected to produce the information requested." *Oglesby*, 920 F.2d at 68. The non-FBI Defendants each searched "'*all* locations likely to contain responsive documents.'" *Huntington v. U.S. Dep't of Commerce*, 234 F. Supp. 3d 94, 103-04 (D.D.C. 2017)(quoting *Bartko v. U.S. Dep't of Justice*, 167 F. Supp. 3d 55, 64 (D.D.C. 2016)). Further, each declaration describes in detail the particular records searched and the search methods used to locate records responsive to the particular request.

Plaintiff cannot not overcome the patent reasonableness of the non-FBI Defendants' searches by speculating that there may be other responsive records that the agencies have not produced. *See, e.g., Batton v.* Evers, 598 F.3d 169, 176 (5th Cir. 2010) (affirming district court's determination that search of locations most likely to hold responsive records was reasonable because "the issue is not whether other documents may exist, but rather whether the search for undisclosed documents was adequate"

(quoting *In re Wade*, 969 F.2d 241, 249 n. 11 (7th Cir. 1992)). Indeed, "[a]n agency's 'failure to turn up a particular document, or mere speculation that as yet uncovered documents might exist,' . . . 'does not undermine the determination that the agency conducted an adequate search for the requested records.'" *Bigwood v. U.S. Dep't of Def.*, 132 F. Supp. 3d 124, 143 (D.D.C. 2015) (citation omitted). Here, any assertion by Plaintiff "that various records related to [its] request must have existed is 'simply conjecture' and is 'insufficient to justifya finding that the search was inadequate.'" *Id.* (citation omitted).

II. DEFENDANTS NSD, NSA, and CIA'S *GLOMAR* RESPONSES WERE PROPER

A *Glomar* response is proper where acknowledging the existence of records would implicate one of the FOIA exemptions. *Gardels,* 689 F.2d at 1103. To justify a *Glomar* response, "[t]he agency must demonstrate that acknowledging the mere existence of responsive records would disclose exempt information." *Elec. Privacy Info. Ctr. v. NSA*, 678 F.3d 926, 931 (D.C. Cir. 2012) (citing *Wolf*, 473 F.3d at 374). But in doing so, the agency's explanatory burden is not demanding, and the standard is, ultimately, no different than in the typical FOIA case: "[A]n agency's justification for invoking a FOIA exemption is sufficient if it appears logical or plausible." *Wolf*, 473 F.3d at 374-75 (quoting *Gardels* at 1105)). "In *Glomar* cases, courts may grant summary judgment on the basis of agency affidavits that contain 'reasonable specificityof detail rather than merely conclusory statements, and if they are not called into question by contradictory evidence in the record or by evidence of agency bad faith.'" *Elec. Privacy Info. Ctr.*,678 F.3d at 931

(quoting *Gardels*, 689 F.2d at 1105). If a *Glomar* response is appropriate, "the agency need not conduct any search for responsive documents or perform any analysis to identify segregable portions of such documents." *PETA v NIH*, 745 F.3d 535, 540 (D.C. Cir.2014).

Glomar responses were issued by the NSD, the NSA, and the CIA, and the explanation for each agency's *Glomar* response is set forth below.

A. NSD's *Glomar* Responses

NSD interpreted Plaintiff's June 18, 2020, request to NSD seeking surveillance records of Edward Butwosky and Matt Couch as seeking NSD records regarding surveillance that, should they exist, would have been authorized under the *Foreign Intelligence Surveillance Act of 1978* (FISA), *codified at* 50 U.S.C. § 1801, *et seq*. As such, NSD asserted and continues to assert, a *Glomar* response to item one of the June 18, 2020 request pursuant to FOIA Exemption 1 as further explained below. [Findlay Declaration, ¶13].

As background, because much of NSD's work is of a classified nature, NSD frequently asserts Exemption 1, protecting properly classified information from disclosure in response to FOIA requests.[3] Information in NSD records is frequently, though not exclusively, classified under section 1.4(c) of Executive Order 13526 which

[3] *See* 5 U.S.C. § 552(b)(1) ("(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant such Executive order.")

covers intelligence activities, sources, and methods.[4] In circumstances where a confirmation that responsive records exist would disclose a classified fact, such as with item one in this request, NSD's usual practice is to assert a *Glomar* response, thereby neither confirming nor denying the existence of information that would disclose or suggest any such fact pursuant to FOIA Exemption 1 and section 3.6(a) of Executive Order 13526.[5] [Findlay Declaration, ¶14].

Section 2.2 of Executive Order 13526 provides for the derivative classification of National Security Information (NSI) by individuals who are not OCAs, including staff of NSD FOIA, through the use of classification guidance. *The United States Department of Justice, National Security Information, Classification Guide* (Ver. 2) (August 22, 2019) ("NSICG") is one such example. NSICG sets forth derivative classification guidance for certain information regularly encountered in NSD FOIA's work. [Findlay Declaration, ¶15].

Several enumerated categories of information in the NSICG, designated for protection under section 1.4(c) of Executive Order 13526, would apply to records responsive to part one of this request, if any such records were to exist. Specifically, such

---

[4] Section 1.4 protects as classified information that "could reasonably be expected to cause identifiable or describable damage to the national security" with subsection c covering "intelligence activities (including covert action), intelligence sources or methods, or cryptology."

[5] "An agency may refuse to confirm or deny the existence or nonexistence of requested records whenever the fact of their existence or nonexistence is itself classified under this order or its predecessors." Exec. Order No. 13526 **§ 3.6(a).**

items would be classified under the NSICG as "an investigative technique requiring a FISA court order or other FISA authorized collection," *see* NSICG, Table 1.10, Item No.INV-4 (a), or because "[t]he fact that a FISA court order or other FISA authorized collection was applied for or obtained in a specific case," s*ee* NSICG, Table 1.10, Item No.INV-8. Consistent with the longstanding treatment of FISA collection as classified, NSD FOIA determined that any FISA-related information responsive to part one of the request would be classified, if it existed, absent some countervailing public disclosure or other action leading to declassification. [Findlay Declaration, ¶16].

The guidance provided in the NSICG is appropriate in requiring the classification of FISA-related records responsive to part one of Plaintiff's request, should they exist, as they would implicate section 1.4 (c) of Executive Order 13526. This is because such disclosure would cause harm to national security as it could permit hostile intelligence services to use FOIA to acquire information about United States intelligence investigations. Once a particular source or method, or the fact of its use in a particular situation, is disclosed, its continued usefulness may be degraded. If NSD were to indicate that it maintains responsive information, such confirmation would provide intelligence analysts of foreign intelligence services with individual pieces of information that could be compiled into a catalogue of FISA activities. Intelligence services and other adversaries could use these disclosures to gain insight into which intelligence agents operating in this country were known to the U.S. Government and which were not. Further, this information could be used to deploy counterintelligence assets against the

U.S. Government thereby impairing U.S. intelligence collection. [Findlay Declaration, ¶17].

Conversely, revealing the absence of responsive records pertaining to particular individuals would tend to indicate that persons within the scope of the request were not targets of surveillance conducted pursuant to FISA. That fact could be extremely valuable to foreign powers and hostile intelligence services who could use it to carry out intelligence activities with some comfort that the U.S. Government is either not monitoring certain people and may not even suspect them or otherwise is not concerned with their activities. [Findlay Declaration, ¶18].

As a result, to protect critical intelligence information and minimize the harm to national security, NSD necessarily asserts a *Glomar* response to requests for information pertaining to operational FISA work. Any such records, were they to exist, would relate to intelligence collection overseen, though not undertaken, by NSD. The existence of such operations is properly classified under section 1.4(c) of Executive Order 13526. Thus, NSD must refuse to confirm or deny whether or not such records exist. [Findlay Declaration, ¶19].

Further, to be credible and effective, absent highly unusual circumstances, NSD must use the *Glomar* response consistently in all cases where the existence of records responsive to a FOIA request is a classified fact, as it is here, including instances in which NSD does not possess records responsive to a particular request. If NSD were to invoke a *Glomar* response only when it actually possessed responsive records, the

Glomar response would be interpreted as an admission that responsive records exist. This practice would reveal the very information that NSD must protect in the interest of national security. An admission of the fact that NSD was in possession of particular records relating to specific FISA-authorized surveillance targets would provide hostile foreign powers with access to additional, operationally valuable information about hypothetical United States intelligence investigations and allow those powers to subvert those same hypothetical investigations. Similarly, if NSD were to make clear to the public via a response to a FOIA request that it did not possess responsive records relating to specific FISA-authorized surveillance targets, hostile foreign powers could benefit from knowledge of this fact. [Findlay Declaration, ¶20].

The determination about the existence or nonexistence of the requested records being classified has not been made to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interests of national security. *See* Exec. Order No. 13526 § 1.7(a). [Findlay Declaration, ¶21].

Thus, NSD properly issued a *Glomar* response to Plaintiff's June 18, 2020, request to NSD seeking surveillance records of Edward Butwosky and Matt Couch pursuant to Exemptions 1 and 3.

B. NSA's *Glomar* Responses

NSA interpreted Plaintiff's June 12, 2020, request to NSA as one seeking intelligence records; specifically, COMINT[6] which includes intercepted foreign government communications. To the extent a Plaintiff seeks intelligence information, NSA's response is to state that it cannot confirm or deny publicly in any case whether or not it has such records, as doing so would reveal whether or not NSA engaged in certain, or any, intelligence activities, and/or did or did not target individual communications for collection. [Kiyosaki Declaration, ¶53].

NSA determined that it could not acknowledge the existence or nonexistence of intelligence information was proper because a positive or negative response to such a request would reveal information that is currently and properly classified in accordance with E.O. 13526 and protected from disclosure by statute, as discussed below. [Kiyosaki Declaration, ¶54].

Exemption 1

Section 552(b)(1) of the FOIA provides that the FOIA does not require the release of matters that are specifically authorized—under criteria established by an Executive Order — to be kept secret in the interest of the national defense or foreign policy and are in fact properly classified pursuant to such Executive Order. The current Executive Order that establishes such criteria is E.O. 13526. [Kiyosaki Declaration, ¶55].

[6] The Kiyosaki Declaration contains a detailed explanation of NSA's system of gathering and analyzing intelligence information. [Kiyosaki Declaration, ¶¶5-10].

Section 1.1 of E.O. 13526 provides that information may be originally classified if: (1) an original classification authority is classifying the information; (2) the information is owned by, produced by or for, or is under the control of the government; (3) the information falls within one or more of the categories of information listed in section 1.4 of the Executive Order; and (4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, and the original classification authority is able to identify or describe the damage. [Kiyosaki Declaration, ¶56].

Section 1.4 of E.O. 13526 provides that information shall not be considered for classification unless it falls within one (or more) of eight specifically enumerated categories of information. The categories of classified information at issue here are found in Section 1.4(c), which includes intelligence activities (including covert action), intelligence sources and methods, or cryptology. Acknowledgment of the existence or nonexistence of operational intelligence information concerning the who, what, when, and how of NSA's SIGINT collection efforts would reveal information that is currently and properly classified as set forth in Sections 1.4(c) of E.O. 13526. [Kiyosaki Declaration, ¶57].

Confirming the existence or nonexistence of responsive records would disclose information that is currently and properly classified TOP SECRET pursuant to Section 1.2(a)(1), of E.O. 13526 because all of the information that Plaintiff sought fall under one or more of the above referenced exceptions and therefore would remain classified to date.

A positive or negative response to Plaintiff's requests reasonably could be expected to cause exceptionally grave damage to national security. Any disclosure of this information could reasonably be expected to harm national security because it would reveal NSA intelligence capabilities, activities, and priorities, which in turn could inhibit SIGINT collection and affect NSA's ability to counter threats to the national security of the United States. [Kiyosaki Declaration, ¶58].

Acknowledging the existence or nonexistence of responsive records on particular individuals or organizations that may be subject to surveillance would provide our adversaries with critical information about the capabilities and limitations of the NSA, such as the types of communications that may be susceptible to NSA detection. Confirmation by NSA that a person's activities are not of foreign intelligence interest or that NSA is unsuccessful in collecting foreign intelligence information on their activities on a case-by-case basis would allow our adversaries to accumulate information and draw conclusions about NSA's technical capabilities, sources, and methods. For example, if NSA were to admit publicly in response to a FOIA request that no information about Persons X or Y exists, but in response to a separate FOIA request about Person Z state only that no response could be made, this would give rise to the inference that Person Z is or has been a target. Over time, the accumulation of these inferences would disclose the targets and capabilities, and therefore the sources and methods, of NSA's SIGINT activities and functions, and inform our adversaries of the degree to which NSA is aware

of some of their operatives or can successfully exploit particular communications. [Kiyosaki Declaration, ¶59].

NSA cannot respond to each case in isolation but must assume that our adversaries will examine all released information together. These compilations of information, if disclosed, could reasonably be expected to cause exceptionally grave and irreparable damage to the national security by providing our adversaries a road map that instructs them on which communication modes or personnel remain safe or are successfully defeating NSA's capabilities. Our adversaries could exploit this information in order to conduct their activities more securely, to the detriment of the national security of the United States. Indeed, section 1.7(e) of E.O. 13526 specifically contemplates the danger of such compilations. [Kiyosaki Declaration, ¶60].

Therefore, the NSA must use the *Glomar* response consistently in all cases where the existence or nonexistence of records responsive to a FOIA request is a classified fact, including in both instances in which the NSA does or does not possess records responsive to a particular request. If the NSA were to invoke a *Glomar* response only when it actually possessed responsive records, the *Glomar* response would be interpreted as an admission that responsive records exist. Consistent use of the *Glomar* response is necessary to ensure its effectiveness. [Kiyosaki Declaration, ¶61].

NSA's determination that the existence or nonexistence of the requested records is classified has not been made to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain

competition; or to prevent or delay the release of information that does not require protection in the interests of national security. [Kiyosaki Declaration, ¶62].

For these reasons, the fact of the existence or nonexistence of intelligence information requested by Plaintiffs is a currently and properly classified matter in accordance with E.O. 13526, and thus Plaintiff's June 12, 2020, FOIA request was properly denied pursuant to FOIA Exemption 1.

Exemption 3

Section 552(b)(3) of the FOIA provides that the FOIA does not require the disclosure of matters that are specifically exempted from disclosure by statute, provided that such statute requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue or establishes particular criteria for withholding or refers to particular types of matters to be withheld. See 5 U.S.C. § 552(b)(3). Review of the application of Exemption 3 consists solely of determining that the statute relied upon qualifies as an Exemption 3 statute, and that the information withheld falls within the scope of the statute. [Kiyosaki Declaration, ¶64].

The information at issue here falls squarely within the scope of several statutes. Information about NSA's SIGINT efforts directly relates to the Agency's core functions and activities and to intelligence sources and methods. Congress enacted three statutes to protect NSA's SIGINT efforts against disclosure, including but not limited to the existence and depth of signals intelligence-related successes, weaknesses, and exploitation techniques. These statutes recognize the vulnerability of signals intelligence

to countermeasures and the significance of the loss of valuable intelligence information to national policymakers, combatant commanders, and the IC. [Kiyosaki Declaration, ¶65].

The first of these statutes is a statutory privilege unique to NSA. NSA's statutory privilege is set forth in Section 6 of the National Security Agency Act of 1959, 50 U.S.C. § 3605. Section 6 of the NSA Act provides that "[n]othing in this chapter or any other law... shall be construed to require the disclosure of the organization or any function of the National Security Agency, or any information with respect to the activities thereof. By this language, Congress expressed its finding that disclosure of any information relating to NSA activities is potentially harmful. Section 6 states unequivocally that NSA cannot be compelled by statute to disclose any information with respect to its activities. Further, while in this case the harm would be exceptionally grave, NSA is not required to demonstrate specific harm to national security when invoking this statutory privilege, rather, NSA need only to show that the information relates to its activities. To invoke this privilege, NSA must demonstrate only that the information it seeks to protect falls within the scope of Section 6. NSA's functions and activities are therefore protected from disclosure regardless of whether or not the information is classified. [Kiyosaki Declaration, ¶66].

The second applicable statute is 18 U.S.C. § 798. This statute prohibits the unauthorized disclosure of classified information: (i) concerning the communications intelligence activities of the United States, or (ii) obtained by the process of communications intelligence derived from the communications of any foreign

government. The term "communication intelligence," as defined by Section 798, means the "procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients." [Kiyosaki Declaration, ¶67].

The third applicable statute is the National Security Act of 1947, as amended by the Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C. § 3024. In particular, section 102A(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 states that "[t]he Director of National Intelligence shall protect the intelligence sources and methods from unauthorized disclosure." NSA, as a member agency of the U.S. IC, must also protect intelligence sources and methods. Like the protection afforded to core NSA activities by Section 6 of the NSA Act of 1959, the protection afforded to intelligence sources and methods is absolute. Whether the sources and methods at issue are classified is irrelevant for purposes of the protection afforded by 50 U.S.C. § 3024. [Kiyosaki Declaration, ¶68].

Congress has enacted these three statutes to protect NSA's SIGINT efforts against disclosure. Given that through these statutes Congress specifically prohibited the disclosure of information related to NSA's functions and activities and its communications intelligence activities, as well as the sources and methods used by the IC as a whole, NSA determined that its SIGINT activities and functions, and its intelligence sources and methods, would be revealed if NSA confirmed or denied the existence of information responsive to Plaintiff's FOIA requests. If NSA were to admit the existence

or nonexistence of the requested records, the very information that Congress authorized NSA to protect would be revealed and this release could show the classified functions, communications intelligence activities, and sources and methods of NSA. [Kiyosaki Declaration, ¶69].

Thus, the acknowledgment of the existence or nonexistence of intelligence information requested by Plaintiff is protected from disclosure by statute pursuant to the following three authorities: (1) Section 6 of the National Security Act of 1959, 50 U.S.C. § 3605, because the information concerns the organization, function, and activities of the NSA as described above; (2) 18 U.S.C. § 798, because disclosure would reveal classified information derived from NSA's exploitation of foreign communications; and (3) Section 1024(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C. § 3024, because the information concerns intelligence sources and methods. For these reasons, acknowledgement of the existence or nonexistence of intelligence information requested by Plaintiffs is prohibited by statute and has been properly determined to be exempt from disclosure pursuant to the FOIA. Accordingly, the *Glomar* response is proper based on Exemption 3 of the FOIA, but this same response is also warranted based on Exemption 1, as set forth above. [Kiyosaki Declaration, ¶70].

C. CIA's *Glomar* Responses

The CIA determined that merely acknowledging the existence or non-existence of records responsive to most portions of Plaintiff's May 28, 2020 and June 18, 2020

requests to CIA would reveal classified or statutorily-protected information within the meaning of FOIA Exemptions 1 and 3. [Blaine Declaration, ¶15].

Exemption 1

Exemption 1 provides that FOIA does not require the production of records that are: "(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order." 5 U.S.C. § 552(b)(1). Consistent with sections 1.1(a) and 3.6(a) of Executive Order 13526,[7] the CIA determined that the fact of the existence or nonexistence or the requested records is currently and properly classified and pertains to "intelligence activities (including covert action), [or] intelligence sources or methods" within the meaning of section 1.4(c) of the Executive Order. [Blaine Declaration, ¶16].

Consistent with Section 1.7 of Executive Order 13526, the CIA's determination that the existence or nonexistence of the requested records is classified has not been made to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interests of national security. [Blaine Declaration, ¶17].

---

[7] Section 1.1(a) sets forth the procedural standards for classification, which have been satisfied in this case. Section 3.6(a) provides that "[a]n agency may refuse to confirm or deny the existence or nonexistence or requested records whenever the fact of their existence or nonexistence is itself classified under this order or its predecessors."

In most cases, upon receipt of a FOIA request, a federal agency will conduct searches for any responsive documents in their holdings and provide the requester with all segregable, non-exempt information contained in those records. In those instances, the fact that records responsive to a given request exist is not itself classified or otherwise exempt. However, in cases such as this one, where a confirmation or denial would itself reveal a classified fact, the Agency routinely asserts a *Glomar* response in order to protect that fact from disclosure. Given the CIA's mandate to collect and analyze foreign intelligence and to conduct counterintelligence, there are many times when the Agency cannot reveal whether or not it possesses records on a particular subject. This is especially the case when substantively responding to a request would tend to show a particular intelligence activity or otherwise reveal previously undisclosed information about CIA sources, capabilities, authorities, interests, relationships with domestic or foreign entities, strengths, weaknesses, and/or resources. Accordingly, in order to maintain the effectiveness of the *Glomar* response, the CIA invokes the response consistently, even where the nonexistence of records appears to be of little consequence. If the Agency answered with a *Glomar* response only in instances where it possesses responsive records, that response could have the effect of confirming the existence of classified information. [Blaine Declaration, ¶18].

The CIA determined that confirming or denying the existence of a responsive record in this particular case, as to certain portions of Plaintiff's requests, could reasonably be expected to cause damage to national security by disclosing intelligence

activities, sources, and methods. There has been no official acknowledgment by the CIA on the topics in the portions of the May 28, 2020, CIA Request or the June 18, 2020, CIA Request for which the CIA offers a *Glomar* response. Disclosing whether or not the CIA possesses the types of information requested in these portions of the requests would provide the CIA's adversaries with details into the Agency's priorities and capabilities, which in turn would impact the CIA's ability to utilize intelligence activities, sources, and methods in the interest of national security. [Blaine Declaration, ¶19].

For example, part 2 of the May 28, 2020, CIA Request seeks "evidence indicating whether the 2016 Data Breach was the result of (1) outside forces (*e.g.*, Russian agents, Pakistani agents, etc.) who hacked the servers from a remote location or (2) an individual or individuals who were present at or inside DNC facilities and copied the data onto a storage device." If the CIA were to confirm the existence of records responsive to this item in the request, such confirmation would show that the Agency devoted resources to this subject and determined the cause of the 2016 data breach. Conversely, if the CIA denied possessing records containing such an assessment, that response would show that the Agency did not determine the cause or did not consider the subject to be of sufficient intelligence interest to warrant analysis or assessment. In either case, disclosing whether or not the CIA possesses responsive records would reveal which topics are the subjects of CIA analysis and study. Such a disclosure would reveal aspects of the Agency's intelligence collection, which itself constitutes an intelligence method. [Blaine Declaration, ¶20].

As another example, parts 4-8 of the May 28, 2020, CIA Request seek records reflecting CIA plans or efforts with journalists, U.S. social media companies, U.S. search engine companies, and entertainment productions. If the CIA were to confirm the existence of responsive records to any of these parts of the request, such confirmation would disclose Agency intelligence activities, sources, and methods. Conversely, if the CIA denied possessing any responsive records, that response would disclose, for example, that the CIA does not have contact with those types of entities. Disclosing this type of information would provide our adversaries with insight into the Agency's sources, relationships, priorities, and capabilities. They could exploit this information by using it to determine how to operate against our national security. [Blaine Declaration, ¶21].

Additionally, part 1 of the June 18, 2020, CIA Request seeks records "reflecting or pertaining to surveillance of Edward Butowsky of Texas or Matt Couch of Arkansas." A primary function of the CIA is to gather intelligence from around the world that can be used by the President and other Government officials in making important decisions. To fulfill this responsibility, the Agency targets certain individuals as part of its foreign intelligence collection efforts. Revealing the identity of a potential foreign intelligence target of collection could cause the exposure of Agency tradecraft, human sources, and specific intelligence interests and activities. As such, confirming or denying the existence of records on any particular individual reasonably could be expected to cause serious damage to national security by indicating whether or not CIA maintained any

human intelligence sources related to an interest in the subject of the request. [Blaine Declaration, ¶22].

In order to avoid the potential for such damage to national security, and to be credible and effective, the CIA must offer a *Glomar* response consistently in cases in which the request is for records on a particular individual with whom the CIA does not have an unclassified affiliation. This approach is necessary in all cases where the existence or nonexistence of records responsive to a FOIA request is a classified fact, including instances in which the CIA does not possess records responsive to a particular request. Otherwise, if the CIA were to assert a *Glomar* response only in cases where responsive records exist, over time the *Glomar* response would serve to identify the particular cases in which the CIA has an intelligence interest in the subject. As a result, the CIA could not effectively offer a *Glomar* response in other cases seeking records on other individuals where the CIA does have a classified interest, including requests seeking information about intelligence sources and targets. This would hinder the CIA's ability to fulfill its intelligence-gathering responsibilities, which reasonably could be expected to cause damage to national security. [Blaine Declaration, ¶23].

For these reasons, the CIA determined that confirming the existence or nonexistence of records responsive to parts 1, 2, 3(3), 4, 5, 6, 7, and 8 of the May 28, 2020, CIA Request, and part 1 of the June 18, 2020, CIA Request reasonably could be expected to cause damage to national security and are therefore currently and properly classified facts exempt from disclosure pursuant to Exemption 1. [Blaine Declaration, ¶24].

Exemption 3

Exemption 3 protects information that is specifically exempted from disclosure by statute. A withholding statute under Exemption 3must: (A) require that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establish particular criteria for withholding or refer to particular types of matters to be withheld. 5 U.S.C. § 552(b)(3).

Section 102A(i)(1) of the National Security Act of 1947, as amended, 50 U.S.C. § 3024 (the "National Security Act"), provides that the Director of National Intelligence ("DNI") "shall protect intelligence sources and methods from unauthorized disclosure." 50 U.S.C. § 3024. Accordingly, the National Security Act constitutes a statute which "requires that the matter be withheld from the public in such a manner as to leave no discretion on the issue." 5 U.S.C. § 552(b)(3). Under the direction of the DNI pursuant to section 102A, and consistent with section 1.6(d) of Executive Order 12333, the CIA is authorized to protect CIA sources and methods from unauthorized disclosure.[8]

As discussed above, the application of Exemption 1, acknowledging the existence or nonexistence of records responsive to parts 1, 2, 3(3), 4, 5, 6, 7, and 8 of the May 28, 2020 CIA Request, and part 1 of the June 18, 2020 CIA Request, would reveal intelligence sources and methods, which the National Security Act is designed to protect.

---

[8] Section 1.6(d) of Executive Order 12333, as amended, 3 C.F.R. 200 (1981), *reprinted in* 50 U.S.C. § 3001 note at 25 (formerly codified at 50 U.S.C.A. § 401 note at 25 (West Supp. 2009)), and as amended by Executive Order 13470, 73 Fed. Reg. 45,323 (July 30, 2008), requires the Director of the CIA to "[p]rotect intelligence and intelligence sources, methods, and activities from unauthorized disclosure in accordance with guidance from the [DNI]."

Accordingly, the fact of the existence or nonexistence of responsive records is exempt from disclosure under Exemption 3 pursuant to the National Security Act. The CIA's *Glomar* response to the above-mentioned parts of Plaintiff's FOIA requests is also grounded in the National Security Act's protection for intelligence sources and methods. As a result, Exemptions 1 and 3 thus apply independently and co-extensively to those parts of the requests. [Blaine Declaration, ¶27].

In contrast to Executive Order 13526, Exemption 3 does not require the CIA to identify and describe the damage to national security that reasonably could be expected to result from confirmation of the existence or nonexistence of the records requested. Nonetheless, the discussion above is applicable here, as well, for a description of the damage to the national security that is reasonably likely to ensue should anything other than a *Glomar* response be provided by the CIA. [Blaine Declaration, ¶28].

III. DEFENDANTS PROPERLY WITHHELD INFORMATION PURSUANT TO FOIA EXEMPTIONS

EOUSA properly withheld information pursuant to FOIA Exemptions 6 and 7(c). NSD properly withheld information pursuant to FOIA Exemption 6. NSA properly withheld information pursuant to FOIA Exemptions 1, 3, and 6. CIA properly withheld information pursuant to FOIA Exemptions 1, 3, 5, 6, 7(C), and 7(E). ODNI properly withheld information pursuant to FOIA Exemptions 1, 3, 5, 6, 7(A), 7(C), 7(D) and 7(E).

The Non-FBI Defendants carefully examined the documents and determined the information withheld from Plaintiff in this case, if disclosed, would reveal, respective to each Exemption, classified information, statutorily protected information, confidential

trade secrets and commercial information, and privileged information; could reasonably be expected to interfere with pending or prospective enforcement proceedings; would cause a clearly unwarranted invasion of the personal privacy, or could reasonably be expected to constitute an unwarranted invasion of personal privacy; could reasonably be expected to disclose the identities of confidential sources and the information they provided; and would disclose techniques and procedures for law enforcement investigations.

Each defendant agency processed all documents responsive to Plaintiff's requests to achieve maximum disclosure consistent with the access provisions of the FOIA. Every effort was made to provide Plaintiff with all material in the public domain and with all reasonably segregable, non-exempt information. The Non-FBI Defendants did not withhold any reasonably segregable, non-exempt portions from Plaintiff.

A. SUMMARY OF FOIA EXEMPTIONS

1. Exemption 1: Classified Information

Exemption 1 protects from disclosure those records that are (a) specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy; and (b) are in fact properly classified pursuant to such Executive Order. 5 U.S.C. § 552 (b)(1). Executive Order 13526 ("E.O. 13526") is the current controlling executive order applicable to the protection of national security information.

2. Exemption 3: Information Protected by Statute

Exemption 3 protects from disclosure information which is specifically exempted from disclosure by statute, provided that the statute requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue. 5 U.S.C. § 552 (b)(3). In weighing the validity of this exemption, a court must first consider whether the statute identified by the agency is in fact a withholding statute, and then whether the withheld material satisfies the statute's criteria. *See CIA v. Sims,* 471 U.S. 159, 167 (1985); *Krikorian v. Dep't of State,* 984 F.2d 461, 465 (D.C. Cir. 1993).

3. *Exemption 5: Privileged Information*

Exemption 5 protects from disclosure inter-agency or intra-agency memorandums or letters that would not be available by law to a party in litigation with the agency. 5 U.S.C. § 552 (b)(5). It ensures that members of the public cannot obtain through FOIA what would ordinarily be protected from disclosure in civil discovery. *See Loving v. Dep't of Def.,* 550 F.3d 32, 37 (D.C. Cir.2008). Among the privileges encompassed by Exemption 5 is the attorney work product doctrine, attorney client privilege, and deliberative process privilege.

The attorney work product doctrine protects materials prepared in anticipation of litigation or for trial by or for another party of its representative. *Judicial Watch, Inc. v. Dep't of Homeland Sec.,* 926 F.Supp.2d 121, 137 (D.D.C. 2013) (quoting Fed.R.Civ.P. 26(b)(3)(A)). The doctrine covers both the mental impressions, conclusions, opinions, or

legal theories of an attorney and factual material prepared in anticipation of litigation. *Tax Analysts v. IRS,* 117 F.3d 607, 620 (D.C. Cir. 1997).

The attorney-client privilege protects confidential communications between an attorney and his or her client relating to a legal matter for which the client has sought professional advice. *Upjohn Co., v. U.S.*, 449 U.S. 383, 389 (1981).

The deliberative process privilege applies to decision making of executive officials generally and protects documents containing deliberations that are part of the process by which government decisions are formulated. *In re Sealed Case*, 121 F.3d 729, 737, 745 (D.C. Cir. 1997). The purpose of the privilege is to prevent injury to the quality of agency decisions by encouraging frank discussions of policy matters, preventing premature disclosure of proposed policies, and avoiding public confusion that may result from disclosure of rationales that were not ultimately grounds for agency action. *Thelen v. Dep't of Justice,* 169 F.Supp.3d 128, 138 (D.D.C. 2016). To fall within the scope of the deliberative process privilege, the material must be both pre-decisional and deliberative. *Coastal States Gas Corp. v. Dep't of Energy,* 617 F.2d 854, 866 (D.C. Cir. 1980). Material is pre-decisional if it was generated before the adoption of an agency policy. *Id.* Material is deliberative if it reflects the give-and-take of the consultive process. *Id.*

4. *Exemption 7(A): Pending Law Enforcement Proceedings*

Exemption 7(A) protects from disclosure records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information could reasonably be expected to interfere with enforcement

proceedings. 5 U.S.C. § 552 (b)(7)(A). The principal purpose of Exemption 7(A) is to prevent disclosures which might prematurely reveal the government's case in court, its evidence or strategies, or the nature, scope, direction, and focus of its investigations, and thereby enable suspects to establish defenses or fraudulent alibis or to destroy or alter evidence. *Maydak v. U.S. Dep't of Justice,* 218 F.3d 760, 762 (D.C. Cir. 2000).

5. Exemptions 6 and 7(C): Unwarranted Invasion of Personal Privacy

Exemption 6 protects from disclosure personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. 5 U.S.C. § 552 (b)(6). Exemption 7(C) similarly protects from disclosure records or information compiled for law enforcement purposed when disclosure could reasonably be expected to constitute an unwarranted invasion of personal privacy. 5 U.S.C. § 552 (b)(7)(C). Exemptions 6 and 7(C) balance individuals' privacy interests in protecting information from disclosure against the public interest in such disclosure. *See generally U.S. Dep't of Justice Reporters Comm. For Freedom of Press*, 489 U.S. 749, 771-76 (1989).

The purpose of Exemption 6 is to "protect individuals from the injury and embarrassment that can result from the unnecessary disclosure of personal information." *U.S. Dep't of State v. Washington Post Co.*, 456 U.S. 595, 599 (1982). The statutory language concerning files "similar" to personnel or medical files has been read broadly by the Supreme Court to encompass any "information which applies to a particular individual . . . sought from government records." *Id.* at 602. The privacy interest in Exemption 6

"belongs to the individual, not the agency." *Amuso v. DOJ*, 600 F. Supp. 2d 78, 93 (D.D.C. 2009).

For purposes of Exemption 7, records are "compiled for law enforcement purposes" if there is "a nexus between the agency's activity . . . and its law enforcement duties." *Keys v. DOJ*, 830 F.2d 337, 340 (D.C. Cir. 1987).

6. Exemption 7(D): Confidential Source Information

Exemption 7(D) protects from disclosure agency records "compiled for law enforcement purposes…by criminal law enforcement authority in the course of a criminal investigation" if release of those records "could reasonably be expected to disclose" the identity of, or information provided by, a "confidential source." 5 U.S.C. § 552 (b)(7)(D); *see also U.S. Dep't of Justice v. Landano,* 508 U.S. 165, 171 (1993).

7. Exemption 7(E): Investigative Techniques and Procedures

Exemption 7(E) protects from disclosure law enforcement records where release "would disclose techniques and procedures for law enforcement investigations or prosecutions or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law." 5 U.S.C. § 552 (b)(7)(E). In order to invoke Exemption 7(E), the Government must make a threshold showing that the materials be records or information compiled for law enforcement purposes. *John Doe Agency v. John Doe Corp.,* 493 U.S. 146, 148 (1989). Law enforcement "techniques and procedures" encompass "how law enforcement officials go about investigating a crime." *Allard K. Lowenstein Int'l Human Rights*

Project v. Dep't of Homeland Sec., 626 F.3d 678, 680-81 (2nd Cir.2010). Defendants are not required to show that the disclosure of information regarding the "techniques and procedures" in question could reasonably be expected to risk circumvention of law as a result of disclosure. *Id.* at 681. Such information is categorically exempt from FOIA disclosure without need for demonstration of harm. *Id.* Exemption 7(E) sets a "low bar for the agency to justify withholding." *Blackwell v. FBI*, 646 F.3d 37, 42 (D.C. Cir. 2011).

B. EXPLANATION OF WITHHOLDING BY EOUSA

Plaintiff's October 26, 2018, request to EOUSA sought criminal records concerning third parties. [ECF No. 5, Exhibit 1]. To the extent that non-public responsive records exist, without consent, proof of death, or an overriding public interest, disclosure of law enforcement records concerning an individual could reasonably be expected to constitute an unwarranted invasion of personal privacy. *See* 5 U.S.C. § 552(b)(6) & (b)(7)(C). Because any non-public records responsive to the request would be categorically exempt from disclosure, EOUSA is not required to conduct a search for non-public records. In this case, instead of a complete third-party denial of records under Exemptions 6 and 7(C), public records were searched and provided to Plaintiff. [Cain Declaration, ¶20].

In this instance, the information being protected from public disclosure consists of third-party names, personal email addresses, and DOJ employee names. Such information provides more insight into said third parties than government activities. There has been

no showing of public interest in the records requested. [Cain Declaration, ¶22].

In applying Exemption 7(C), the court "balance[s] the privacy interests that would be compromised by disclosure against the public interest in release of the requested information." *Davis v. U.S. Dep't of Justice*, 968 F.2d 1276, 1281 (D.C. Cir. 1992). Courts recognize that there is considerable stigma inherent in being associated with law enforcement proceedings, and accordingly "do [ ] not require a balance tilted emphatically in favor of disclosure" when reviewing 7(C) exemption claims. *Bast v. Dep't of Justice*, 665 F.2d 1251, 1254 (D.C. Cir.1981). [Cain Declaration, ¶24].

For purposes of both Exemptions 6 and 7(C), the information that is being withheld consists of third-party information and DOJ employee names. [Cain Declaration, ¶25].

Public identification of government personnel involved in criminal investigations could subject them to harassment both in the conduct of their official duties and their private lives. Similarly, individuals - whether targets, suspects, or witnesses - have a strong interest in not being unfairly associated publicly with alleged criminal activity. The mention of a private individual's name in a law enforcement file engenders comment and speculation and could produce an unfair stigma which could expose the individual to harassment or criticism. In the underlying matter in particular, several measures were taken by the court to seal pleadings to protect third parties and to prevent harassment of the associated families. [Cain Declaration, ¶26].

These individuals also have a substantial privacy interest in avoiding disclosure of their personal information in the requested documents. For purposes of both Exemptions 6 and 7(C), the release of personally identifiable information could subject the users to an unwarranted invasion of their personal privacy by leading to efforts to contact them directly, gain access to their personal information, or subject them to harassment or harm. There is no countervailing public interest that warrants the release of an individual's personally identifiable information, and its dissemination would not help explain the government's activities or operations. The need to protect an individual's privacy rights far outweighs any public need for the disclosure of the users' personally identifiable information. A release of records via FOIA is not just a release to Plaintiff, but constructively, a release to the world. Even a diminished privacy interest would outweigh the absence of any cognizable public interest identified by Plaintiff. [Cain Declaration, ¶27].

The information protected under Exemptions 6 and 7(C) is described in the *Vaughn* Index, attached as Exhibit A to the Cain Declaration.

C. EXPLANATION OF WITHHOLDING BY NSD

Plaintiff's June 15, 2020, request to NSD sought records concerning the DNC email hack. [ECF No. 5, Exhibit 8]. In response, NSD redacted, and thus withheld, the names and contact information, including e-mail addresses and direct telephone numbers, of non-Senior Executive Service (SES) Executive Branch personnel engaged in their

official duties. NSD withheld this information pursuant to FOIA Exemption 6. [Findlay Declaration, ¶22].

Though it is the general practice, NSD does not always redact such names. In this case, NSD balanced the privacy interests of the Executive Branch personnel identified in the documents, including their interests in avoiding publicity regarding aspects of their work, against the public interest in the disclosure of this information. NSD has assessed that the legitimate public interest in the names and contact information of particular employees is minimal in this context because this information would not shed any meaningful light on NSD's or the Department's operations. As a result, NSD determined that the privacy rights of these individuals outweighed the public interest, if any, in the disclosure of the information. NSD determined, therefore, that releasing this information would constitute a clearly unwarranted invasion of these individuals' privacy which outweighs the public interest in disclosure. [Findlay Declaration, ¶23].

A copy of the redacted documents produced to Plaintiff is attached as Exhibit G to the Findlay Declaration.

D. EXPLANATION OF WITHHOLDING BY NSA

Plaintiff's October 29, 2018, request to the NSA sought Congressional correspondence with various third parties. [ECF No. 5, Exhibit 2]. In response, the NSA conducted a search for responsive records and provided to Plaintiff five partially-redacted

records, totaling 13 pages, and withheld six records in their entirety, totaling 16 pages, pursuant to FOIA Exemptions 1, 3, and 6.[9] [Kiyosaki Declaration, ¶12].

Exemption 1 Redactions

Section 552(b)(1) of the FOIA provides that the FOIA does not require the release of matters that are specifically authorized—under criteria established by an Executive Order—to be kept secret in the interest of the national defense or foreign policy and are in fact properly classified pursuant to such Executive Order. The current Executive Order that establishes such criteria is E.O. 13526. [Kiyosaki Declaration, ¶24].

Section 1.1 of E.O. 13526 provides that information may be originally classified if: (1) an original classification authority is classifying the information; (2) the information is owned by, produced by or for, or is under the control of the government; (3) the information falls within one or more of the categories of information listed in section 1.4 of the Executive Order; and (4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, and the original classification authority is able to identify or describe the damage. [Kiyosaki Declaration, ¶25].

Section 1.4 of E.O. 13526 provides that information shall not be considered for classification unless it falls within one (or more) of eight specifically enumerated categories of information. The categories of classified information at issue here are found

[9] As previously noted, the initial application of Exemption 5 was later deemed inappropriate, but the information was properly redacted under other FOIA exemptions.

in Section 1.4(c), which includes intelligence activities (including covert action), intelligence sources and methods, or cryptology. [Kiyosaki Declaration, ¶26].

The release of the redacted material would disclose information that is currently and properly classified TOP SECRET pursuant to Section 1.2(a)(1) of E.O. 13526, because the information could reasonably be expected to cause exceptionally grave damage to the national security. Any disclosure of this information would obviously and immediately affect the ability of NSA to counter threats to the national security of the United States. [Kiyosaki Declaration, ¶27].

NSA reviewed the categories of redacted information pursuant to this FOIA request and determined that those categories are currently and properly classified in accordance with E.O. 13526. Based on that determination, NSA further determined that the responsive material at issue was properly redacted, as this information is currently and properly classified in accordance with E.O. 13526. Accordingly, the release of this intelligence information could reasonably be expected to cause exceptionally grave damage to the national security. The damage to national security that reasonably could be expected to result from the unauthorized disclosure of this classified information is described below. Finally, in accordance with Section 1.7 of E.O. 13526, no information was classified or withheld in order to conceal violation of law, or to prevent embarrassment to the Agency. [Kiyosaki Declaration, ¶28].

Here, the redacted information is currently and properly classified. [10] In fact, these redactions protect information that is classified as TOP SECRET, underscoring the exceptionally grave damage that would be implicated by its release. These redactions protect specific information concerning and derived from NSA SIGINT reporting, which plainly cannot be released to the public without exceptionally grave damage to national security. This redacted information, if revealed, would show specific topics that are the subject of NSA SIGINT reports. These intelligence reports are some of the most closely held and protected products that NSA creates and cannot be disclosed without risk to national security given the insights they provide. [Kiyosaki Declaration, ¶29].

Exemption 3 Redactions

Section 552(b)(3) of the FOIA provides that the FOIA does not require the disclosure of matters that are specifically exempted from disclosure by statute, provided that such statute requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue or establishes particular criteria for withholding or refers to particular types of matters to be withheld. See 5 U.S.C. § 552(b)(3). Review of the application of this section of the FOIA consists solely of determining that the statute relied upon qualifies as an exempting statute under Exemption 3 and that the information withheld falls within the scope of the statute. No showing of national security harm is

[10] Exemption 1 is cited on Bates stamp pages TTP NSA 000007 and TTP NSA 000013. see Kiyoski Declaration, Exhibit E at 7, 13. NSA's response to QFR 1 1 on Bates Stamp page TTP NSA 000005 is also classified, despite the absence of a (b)(l) citation.

required in order to maintain a proper exemption pursuant to Exemption 3. [Kiyosaki Declaration, ¶30].

The redacted material subject to Exemption 3 plainly falls within NSA's unique statutory privilege: Section 6 of the National Security Agency Act of 1959, 50 U.S.C. § 3605. As noted, Section 6 is a statutory privilege unique to NSA and provides that "[n]othing in this chapter or any other law. . . shall be construed to require the disclosure of the organization or any function of the National Security Agency, or any information with respect to the activities thereof, or of the names, titles, salaries, or number of the persons employed by such agency." By this language, Congress expressed its finding that disclosure of any information relating to NSA activities is potentially harmful. The protection provided by this statute is, by its very terms, absolute, as Section 6 states unequivocally that, notwithstanding any other law, including the FOIA, NSA cannot be compelled to disclose any information with respect to its activities. Further, NSA is not required to demonstrate specific harm to national security when invoking this statutory privilege, rather, NSA need only to show that the information falls within the scope of Section 6. NSA's organization, functions, activities, and nonpublic personnel are therefore protected from disclosure regardless of whether or not the information is classified. [Kiyosaki Declaration, ¶31].

Here, NSA has redacted certain information relating to NSA's functions and activities pursuant to Exemption 3.[11] As explained, these redactions protect information concerning and derived from NSA SIGINT reporting. Collecting intelligence information and providing it to principals, advisors, and leaders in the United States government, including Congressional oversight committees, is a core function and primary activity of NSA. Additionally, these redactions protect information revealing NSA's intelligence assessments, another central function and activity of NSA. Finally, these redactions protect information describing NSA's role in the Vulnerabilities Equities Process ("VEP") that have not been publicly acknowledged. The details of NSA's involvement in the VEP are also an NSA function/activity. Congress's intent with respect to the protection of NSA's organization, functions, and activities is manifest by the plain language of Section 6; where, as here, the disclosure of the requested information would improperly reveal aspects of NSA's mission, the invocation of Exemption 3 pursuant to this statute is proper. [Kiyosaki Declaration, ¶32].

NSA also redacted the standard identifier of an NSA employee pursuant to Exemption 3. NSA employees' standard identifiers contain some or all of a particular employee's name. NSA protects the standard identifiers of its personnel pursuant to

[11] Exemption 3 is cited on Bates stamp pages TTP NSA 00001, 000002, 000003, 000007 and 000013. see Kiyosaki Declaration, Exhibit E at 1, 2, 7, 13. NSA's responses to QFR 1 1, 12, and 13 on Bates stamp pages TTP NSA 000005 and TTP NSA 000006 are also protected by Exemption 3 pursuant to Section 6, despite the absence of a (b)(l) citation.

Section 6, which, as noted, protects from disclosure the organization of NSA and the names and titles of those employed with NSA. This material is appropriately redacted pursuant to Exemption 3 of the FOIA, as it reflects information that squarely falls within the express protections of Section 6. [Kiyosaki Declaration, ¶33].

Exemption 6 Redactions

Lastly, section 552(b)(6) of the FOIA protects from disclosure information whose release would lead to a clearly unwarranted invasion of personal privacy. In order to determine whether material is properly withheld pursuant to this exemption, an agency must conduct a balancing test, weighing the public interest in disclosure versus the privacy interest at stake. [Kiyosaki Declaration, ¶35].

Here, a careful examination of the redacted material reveals that the public interest in disclosure is minimal and clearly outweighed by the privacy interest involved. Specifically, the only material redacted pursuant to Exemption 6 contains the full names and phone numbers of members of the SSCI staff. There is no public interest in the release of these staff members' personal information, specifically their names and phone numbers. These individuals have an obvious privacy interest in their personal information. [Kiyosaki Declaration, ¶36].

In addition to the redacted material on the five documents released in part, NSA also entirely withheld from disclosure six documents, totaling 16 pages, pursuant to Exemptions 1 and 3. Most, if not all, of this material is classified and non-segregable for

that reason alone, as described in further detail below, and thus NSA is unable to produce any non-exempt portions of the responsive materials. [Kiyosaki Declaration, ¶37].

Exemption 1 Withheld in Full

As explained above, section 552(b)(1) of the FOIA provides that the FOIA does not require the release of matters that are specifically authorized—under criteria established by an Executive Order—to be kept secret in the interest of the national defense or foreign policy and are in fact properly classified pursuant to such Executive Order. The current Executive Order that establishes such criteria is E.O. 13526. [Kiyosaki Declaration, ¶38].

The release of the material withheld in full would disclose information that is currently and properly classified TOP SECRET pursuant to Section of E.O. 13526, because the information could reasonably be expected to cause exceptionally grave damage to the national security. Any disclosure of this information would obviously and immediately affect the ability of NSA to counter threats to the national security of the United States. [Kiyosaki Declaration, ¶41].

NSA reviewed the categories of redacted information pursuant to this FOIA request and determined that those categories are currently and properly classified in accordance with E.O. 13526. Based on that determination, NSA further determined that the responsive material at issue was properly withheld, as all of this information is currently and properly classified in accordance with E.O. 13526. Accordingly, the release of this information could reasonably be expected to cause exceptionally grave damage to

the national security. The damage to national security that reasonably could be expected to result from the unauthorized disclosure of this classified information is described below. Finally, in accordance with Section 1.7 of E.O. 13526, no information was classified or withheld in order to conceal violation of law, or to prevent embarrassment to the Agency. [Kiyosaki Declaration, ¶42].

All of the documents withheld in full by NSA are currently and properly classified. In fact, all of these documents are classified TOP SECRET,[12] underscoring the exceptionally grave damage that would be implicated by their release. Moreover, NSA determined that the classified material withheld in full does not contain meaningfully segregable information that could be released to the public. This is so for several reasons. First, in many instances, the withheld material does not contain any non-classified material. Second, even in those documents where there are stray lines containing unclassified or U//FOUO material, that material, without more, is not meaningful or substantive. Finally, these documents concern specific topics the very existence of which are classified. While NSA is prepared to state, on the public record, that it has withheld a specified number of materials responsive to Plaintiffs request, namely, "correspondence received from or sent to any member of Congress (or anyone representing a member of

[12] In fact, many of these documents have additional classifications indicating the sensitivity of the material at issue. For example, many of the documents are marked with "ORCON" designator, indicating that the originator of the information controls to whom it is release. Additionally, all of the documents contain the designator "NOFORN," indicating that the information may not be released to foreign governments, foreign nationals, or non-U.S. citizens without permission of the originator and in accordance with DNI policy.

Congress or Congressional committee) since January 1, 2016 regarding or referencing" either Seth Conrad Rich, Julian Assange, Wikileaks, Kim Dotcom, Aaron Rich, Shawn Lucas, Kelsey Mulka, Imran Iwan, Abid Awan, Jamal Awan, Hina Alvi, or Rao Abbas, it cannot provide additional detail concerning the withheld material without risking exceptionally grave damage to national security. [Kiyosaki Declaration, ¶43].

These documents contain information from intelligence reporting derived from SIGINT and associated analysis or explanation, which plainly cannot be released to the public without exceptionally grave damage to national security. The information from these intelligence reports, which are some of the most closely held and protected products that NSA creates, cannot be disclosed without risk to national security given the insights they provide. [Kiyosaki Declaration, ¶44].

All the documents withheld in full by NSA are classified at levels which, on their face, indicate the sensitivity of the at-issue material. Moreover, this classified material does not contain meaningfully segregable portions, and, in most instances the very existence of the specific material withheld is classified. Accordingly, while NSA may, without harm to national security, publicly state that it possesses material responsive to Plaintiffs FOIA request, it does not follow from that admission that NSA must in turn reveal classified details concerning such material. [Kiyosaki Declaration, ¶45].

Exemption 3 Withheld in Full

While, for the aforementioned reasons, the materials withheld in full are currently and properly classified and accordingly exempt from disclosure pursuant to Exemption 1,

the Court need not consider the classification issue, as all requested records are concurrently exempt pursuant to Exemption 3. 5 U.S.C. § 552(b)(3). [Kiyosaki Declaration, ¶46].

The information withheld in full here is protected from disclosure by several statutes. First and foremost, the withheld documents concern or reference NSA SIGINT information, which implicate both the Agency's core functions and activities, as well as intelligences sources and methods. As such, they fall squarely within NSA's unique statutory privilege: Section 6 of the National Security Agency Act. Congress enacted this statute to protect the fragile nature of NSA's SIGINT efforts, including, but not limited to, the existence and depth of signal intelligence-related analytical successes, weaknesses, and exploitation techniques. This statute recognizes the vulnerability of SIGINT to countermeasures and the significance of the potential loss of valuable intelligence information to national policymakers, combatant commanders, and the IC. [Kiyosaki Declaration, ¶48].

In addition to the plainly applicable statutory framework of Section 6, the materials withheld in full also are protected from disclosure by 18 U.S.C. § 798. This statute prohibits the unauthorized disclosure of classified information: (i) concerning the communication intelligence activities of the United States, or (ii) obtained by the process of communication intelligence derived from the communications of any foreign government. The term "communication intelligence," as defined by Section 798, means the "procedures and methods used in the interception of communications and obtaining

the information from such communications by other than the intended recipients." 18 U.S.C. § 798(b). As noted above, some of the withheld material implicates NSA's SIGINT information. This material, while classified, is also plainly protected by the strictures of § 798. This statutory scheme underscores Congress's commitment to protecting communication intelligence, which is central to NSA's mission, from disclosure. Here, given the classified nature of the withheld material, as well as its reflection of NSA's core activities, it is axiomatic that disclosure of the withheld information about this intelligence source (communication intelligence) and the related methods used to secure it, would reveal critical information about the means through which NSA collects and processes communication intelligence, plainly falling within the scope of this statutory scheme. [Kiyosaki Declaration, ¶50].

Finally, the withheld material is protected from disclosure by Section 102a(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C. § 3024, which states that "[t]he Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure." NSA, as a member agency of the U.S. IC, must also protect intelligence sources and methods. Like the protection afforded to core NSA activities by Section 6 of the NSA Act of 1959, the protection afforded to intelligence sources and methods is absolute. Whether the sources and methods at issue are classified is irrelevant for purposes of the protection afforded by 50 U.S.C. § 3024. [Kiyosaki Declaration, ¶51].

Here, the details of the withheld material responsive to Plaintiff's request concerning correspondences with Congress regarding or referencing specific individuals implicates critical sources and methods. Detailed discussions about circulated intelligence reports and NSA capabilities, both of which generally describe the type of information present in these withheld materials, reflect the very sources and methods this statute is designed to protect. [Kiyosaki Declaration, ¶52].

Thus, the records withheld in full are not only exempt from disclosure due to their classified nature, but also, in light of the fact that their contents are plainly protected from release by the aforementioned three statutory authorities: (1) Section 6, 50 U.S.C. § 3605, because the withheld information concerns the core function and/or activities of NSA; (2) 18 U.S.C. § 798, because disclosure could reveal classified information derived from NSA's exploitation of foreign communications; and (2) Section 2A(i)(1), 50 U.S.C. § 3024, because the information concerns intelligence sources and methods. For these reasons, all of the documents withheld in full are, in the alternative, protected from disclosure pursuant to Exemption 3. [Kiyosaki Declaration, ¶53].

E. EXPLANATION OF WITHHOLDINGS BY CIA[13]

Plaintiff's May 28, 2020, request to CIA, parts 3(1) and 3(2) sought records related to a task force investigating Russian collusion with Trump affiliates. [ECF No. 5, Exhibit 3]. In response, CIA withheld six documents in full pursuant to FOIA

[13] The CIA consulted with the FBI regarding three pages of CIA records, and the FBI asserted withholdings pursuant to FOIA Exemptions 6, 7(C), and 7(E). The basis for FBI's withholdings is explained in the Third Declaration of Michael G. Seidel.

Exemptions 1, 3, 5 and 6. [Blaine Declaration, ¶12, Exhibit G]. Plaintiff's June 18, 2020, request, part 2 to CIA sought records pertaining to David Petraeus. [ECF No. 5, Exhibit 9]. In response, CIA released in part four documents and withheld in full 157 documents pursuant to FOIA Exemptions 1, 3, 5, 6, 7(C), and 7(D). [Blaine Declaration, ¶13, Exhibit G].

Exemption 1

The information withheld by CIA pursuant to Exemption 1 is classified information that is owned by and is under the control of the U.S. Government. The information falls under classification category § 1.4(c) of the Executive Order because it concerns "intelligence activities (including cover action), [or] intelligence sources and methods." Further, its unauthorized disclosure could reasonably be expected to result in damage to national security. In addition, in accordance with § 1.8(a) of the Order, none of the information at issue has been classified in order to conceal violations of law, inefficiency or administrative error; prevent embarrassment to a person, organization or agency; restrain competition; or prevent or delay the release of information that does not require protection in the interest of national security. Furthermore, the responsive records that contain CIA classified information are properly marked in accordance with § 1.6 of the Executive Order. [Blaine Declaration, ¶33].

Here, the information withheld pursuant to Exemption 1 consists of (i) identifying information regarding covert personnel; (ii) identifying information regarding covert

locations; and (iii) information that would tend to reveal specific intelligence sources, methods, and or activities. [Blaine Declaration, ¶34].

Covert Personnel. The CIA considers the identities of its covert employees and their activities to constitute intelligence sources and methods. In order to carry out its mission of gathering and disseminating intelligence, the CIA places certain employees under cover to protect the fact, nature, and details of the Agency's interest in foreign activities as well as the intelligence sources and methods employed to assist in those activities. Disclosing the identity of a covert employee could expose the intelligence activities with which the employee has been involved and the sources with whom the employee has had contact. Additionally, disclosing the identity of a covert employee could jeopardize the safety of the employee, his or her family, his or her sources, and even other persons with whom he or she has had contact. In order for the Agency to carry out effectively its foreign-intelligence gathering mission, it is imperative that the identities of these covert personnel be protected. [Blaine Declaration, ¶35].

Covert Locations. The records at issue also contain details related to covert CIA locations. The places where the CIA maintains a presence constitute classified intelligence methods of the Agency. The CIA's covert overseas facilities are critical to the CIA's mission, as they provide a base for the CIA's foreign intelligence activities. Acknowledging the location of such covert facilities can endanger the physical safety of covert CIA officers who work at those locations by, among other things, significantly

increasing the likelihood that those facilities could be targeted for attacks. [Blaine Declaration, ¶36].

Intelligence Methods and Activities. The documents at issue also contain information concerning CIA intelligence methods as well as details of specific intelligence activities. [Blaine Declaration, ¶37].

The CIA must guard against the disclosure of the clandestine methods it uses to collect and analyze intelligence. Intelligence methods are the techniques and means by which an intelligence agency accomplishes the mission, and the classified internal regulations, approvals, and authorities that govern the conduct of CIA personnel. In this case, the CIA withheld information related to the methods that it uses to collect and analyze intelligence. This includes certain classified details regarding the Agency's information technology and security of those systems. [Blaine Declaration, ¶38].

The manner in which the Agency protects its intelligence on its information systems is itself a method—indeed, one that is critical to the CIA's mission of collecting and analyzing foreign intelligence. Disclosure of different details regarding the Agency's information technology and information security may complicate or completely disrupt CIA communications. For example, a disruption to the Agency's computer network could hinder active operations or allow for the interception of classified communications by adversaries. The Agency must protect identifying information regarding its information systems, its information security protocols, and details regarding its technical capabilities concerning this information systems from disclosure. The Agency must do

so in order to prevent adversaries, terrorist organizations, and others from learning about how the CIA operates, which would allow them to use countermeasures to undermine U.S. intelligence capabilities and render collection efforts ineffective. [Blaine Declaration, ¶39].

For all of these reasons, the CIA cannot disclose these types of details in the responsive records insofar as they would disclose intelligence sources, methods, and activities. The CIA has determined that this information remains currently and properly classified pursuant to the criteria of Executive Order 13526 as its disclosure could reasonably be expected to cause damage to national security. [Blaine Declaration, ¶40].

Exemption 3

Exemption 3 protects information that is specifically exempted from disclosure by statute. Section 102A(i)(1) of the National Security Act,[14] and Section 6 of the Central Intelligence Agency Act of 1949, as amended, 50 U.S.C. § 3507 (the "CIA Act") constitute withholding statutes in accordance with Exemption 3. Both have been widely recognized as such, and both apply here to protect certain information in the records from disclosure. [Blaine Declaration, ¶41].

National Security Act

In conjunction with the National Security Act, Exemption 3 applies co-extensively to all the information protected by Exemption 1 because the information would reveal

[14] Background information on the National Security Act is provided in Part III.B of the Blaine Declaration.

specific intelligence sources and methods. Additionally, there are some aspects of the Agency's intelligence sources and method that are unclassified but would nevertheless reveal intelligence sources and methods protected by the National Security Act if disclosed. This includes some details related to the Agency's information technology systems. This information would show the types of equipment relied upon by Agency personnel to carry out the CIA's objectives. The National Security Act applies to protect this information. [Blaine Declaration, ¶42].

The National Security Act also applies here to protect under Exemption 3 two additional categories of information: (i) classification and dissemination control markings, and (ii) code words and pseudonyms. [Blaine Declaration, ¶43].

Classification and Dissemination Control Markings. The records at issue contain classification and dissemination-control markings, which are among the intelligence methods used to control the dissemination of intelligence-related information and to protect such information from unauthorized disclosure. These markings indicate the overall classification level as well as the classification of discrete portions of a document, the presence of any compartmented information, and the limits on disseminating the information. The markings reveal details about the sensitivity and content of the underlying intelligence and indicate restrictions on access or handling. Disclosure of these markings would reveal or highlight areas of particular intelligence interest, sensitive collection sources or methods, foreign sensitivities, and procedures for gathering, protecting, and processing intelligence. [Blaine Declaration, ¶44].

Code Words and Pseudonyms. Some of the records at issue contain code words and pseudonyms. The use of code words is an intelligence method whereby words and letter codes are substituted for actual names, identities, or programs in order to afford additional protection to intelligence sources and other intelligence methods. Specifically, the CIA and other federal agencies use code words in cables and other correspondence to disguise the true name of a person or entity of operational intelligence interest, such as a source, a foreign liaison service, or a covert program. The CIA also uses pseudonyms, which are essentially code names, in many of its internal communications. [Blaine Declaration, ¶45].

When obtained and matched to other information, code words and pseudonyms possess a great deal of intelligence value to someone able to fit them into the proper framework. For example, the reader of a message is better able to assess the nature of a piece of intelligence if the reader can identify a location, an undercover employee, an intelligence activity, or a foreign activity by the code word or pseudonym. By using these code words, the CIA and other federal agencies add an extra measure of security, minimizing the damage that would flow from an unauthorized disclosure of intelligence information. The disclosure of code words and pseudonyms—especially in context, or in the aggregate—can permit foreign intelligence services and other adversaries to fit disparate pieces of information together and to discern or deduce the identity or nature of the person or project for which the code word or pseudonym stands. [Blaine Declaration, ¶46].

Although no harm rationale is required under Exemption 3, for the reasons discussed in this section, the release of the information withheld under Exemption 3 pursuant to the National Security Act could result in harm by significantly impairing the CIA's ability to carry out its core missions of gathering and analyzing foreign intelligence. [Blaine Declaration, ¶47].

Central Intelligence Act

Section 6 of the CIA Act protects "the organization, functions, names, official titles, salaries, or numbers of personnel employed by the Agency" from disclosure. 50 U.S.C. § 3507. The CIA Act therefore constitutes a federal statute that "establishes particular criteria for withholding or refers to particular matters to be withheld." 5 U.S.C. § 552(b)(3). The CIA Act applies to protect the listed information of both CIA officers and contractors. [Blaine Declaration, ¶48].

Pursuant to the CIA Act, here, the Agency withheld names and other personally-identifying information of Agency personnel, such as Agency identification numbers, telephone numbers, email addresses, locations, and core job functions. This is precisely the type of identifying information the CIA Act protects against disclosure. Although no harm rationale is required, disclosure of the information withheld would expose the identities of CIA personnel, and possibly their job duties and contact information, which could subject them to harassment, embarrassment, or unwanted contact. Disclosure would also highlight the capabilities and possible limitations of the Agency's intelligence

activities, which could hinder the Agency's efforts to fulfill its intelligence-gathering mission. [Blaine Declaration, ¶49].

Exemption 5

As a preliminary matter, the CIA Final Response Letter indicated that the CIA withheld information under Exemption 5 in the documents responsive to parts 3(1) and 3(2) of the May 2020 CIA Request, and part 2 of the June 2020 CIA Request. [Blaine Declaration, Exhibit G]. The CIA is no longer asserting Exemption 5 in relation to the documents responsive to parts 3(1) and (3)(2) of the May 2020 CIA Request. This does not alter the fact that each of the documents responsive to that request were properly withheld in full pursuant to other FOIA exemptions as addressed in this declaration. [Blaine Declaration, ¶50].

The CIA continues to assert Exemption 5 in relation to the documents responsive to part 2 of the June 2020 CIA request. All of the information that the Agency withheld under Exemption 5 has been circulated either within the Agency or with other agencies within the federal government, and therefore satisfies the intra- and inter-agency threshold of the exemption. As described in the CIA's *Vaughn* Index, the information for which Exemption 5 was asserted applies to discussions that are protected by the deliberative process privilege, the attorney work-product privilege, or the attorney-client privilege. [Blaine Declaration, ¶51].

Deliberative Process Privilege

The CIA invoked the deliberative process privilege here for the majority of the records responsive to part 2 of the June 2020 CIA Request, which is the request for records concerning whether former CIA Director Petraeus mishandled classified information. As a preliminary matter, none of the records at issue were created 25 years or more before the date of the request. Further, as noted in the *Vaughn* Index, many of the records consist of OIG investigation case progress reviews, logs of investigative activity, correspondence with DOJ regarding deliberations at different stages of the investigation, and witness interview notes. Each of these communications reflect the CIA's internal and confidential decision-making process at interim stages of the investigation related to former CIA Director Petraeus. Some of the documents withheld are draft versions, which were not finalized, contain no date, or have no signature. Also, some of these drafts have embedded comments or contain recommendations and edits, as well as discussions about wording, accuracy, and other deliberative ancillary matters. These communications do not convey final Agency viewpoints on a particular matter, but rather reflect different considerations, opinions, options, and approaches that preceded the Department of Justice's final decision to pursue prosecution. [Blaine Declaration, ¶53].

The Agency invoked the deliberative process privilege to protect certain investigatory documents compiled by the CIA's OIG. The documents include case reviews and updates, interview notes, and internal communications. The documents

reflect the status and direction of the investigation at a given point in time, which was subject to change as new information was acquired. For example, as investigators conducted interviews, the information offered by those interviewed provided new leads that changed or expanded the scope of the investigation, prompted investigators to focus on certain individuals, or conversely, foreclosed other avenues of inquiry. Similarly, the types of records collected and questions posed by the investigators reveal their thought processes by showing precisely what information they considered during the course of the investigation. As a result, the documents withheld in full or in part pursuant to the deliberative process privilege do not reveal a final decision, but reflect the investigative, deliberative process that the Agency undertook. If one compared the information gathered during the investigation (documented in the withheld records) against the publicly-filed documents related to this investigation (such as the signed plea agreement), it would permit one to determine which details investigators did not consider significant or what weight they accorded certain sources. It would also reveal that some of the information compiled was not utilized or selected for inclusion in the final analysis, which ultimately would open the Agency's deliberative process to public scrutiny on decisions that were not final. This, in turn, would chill the free flow of discussion in agency decision-making. [Blaine Declaration, ¶54].

The CIA has determined that, to the extent the documents contain any factual material, that content is part and parcel of the deliberations, and its disclosure would expose or cause harm to the Agency's deliberations. The disclosure of facts in these

documents would reveal the nature of the preliminary recommendations and opinions preceding the final determinations. In the case of draft documents, disclosure of these records would allow for the comparison between the wording in the final version and the drafts thereby revealing what information was considered significant or was discarded in the course of the drafting process. Disclosure of any of these documents would inhibit the frank communications and free exchange of ideas that the privilege is designed to protect. If the withheld information were released, CIA employees may hesitate to offer their candid opinions to superiors or coworkers, and such self-censorship would tend to degrade the quality of Agency decisions. Additionally, revealing this information could mislead or confuse the public by disclosing rationales that did not form the basis for the Agency's final decisions. [Blaine Declaration, ¶55].

Attorney Work-Product Privilege

Additionally, the Agency asserted the attorney work-product privilege to protect eight documents under Exemption 5. The privilege was invoked to withhold communications from or between Agency attorneys discussing the then-ongoing investigation, legal issues, and deliberations regarding the future progression of the investigation. All of the communications withheld as attorney work product were created in reasonable anticipation of litigation; namely, a criminal prosecution. If this information were to be released, it would expose the various attorneys' work to scrutiny and reveal preliminary litigation risk analysis and strategy. This is the type of

information that the attorney work-product privilege is designed to protect. [Blaine Declaration, ¶56].

Attorney-Client Privilege

In this case, the CIA asserted the attorney-client privilege regarding one document to protect confidential communications between senior Agency officials and senior attorneys within the CIA's Office of General Counsel. In the one document at issue, an Agency official requested legal advice related to information concerning the FBI investigation and a certain proposed course of action. The confidential communications consist of factual information supplied by the client in connection with the request for legal advice, as well as discussions between attorneys that reflect those facts, and legal analysis and advice provided to the client. The confidentiality of these communications was maintained. If this confidential information were to be disclosed, it would subject the legal guidance to scrutiny and reveal preliminary legal risk analysis and strategy. This is the type of information that the attorney-client privilege is designed to protect. [Blaine Declaration, ¶57].

Exemption 6

Exemption 6 provides that the FOIA's information release requirements do not apply to "personnel and medical files and similar files, the disclosure of which could constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(6). The term "similar files" covers any personally identifying information of covert and overt CIA personnel and other individuals mentioned in the documents, such as names,

positions, contact information, social security numbers, unique Agency identifiers (such as pseudonyms and Agency identification numbers), and similar identifying details. [Blaine Declaration, ¶58].

In response to the parts of the May 2020 CIA Request and the June 2020 CIA Request that the Agency processed, the Agency withheld identifying information of the individuals involved in the topics at issue. The individuals named in the records are CIA employees, non-agency government personnel, and other third parties unaffiliated with the Agency. These persons maintain a strong privacy interest in this information because its release could subject them to harassment, embarrassment, or unwanted contact by virtue of their association with the subject matters of the FOIA requests. [Blaine Declaration, ¶60].

Conversely, Plaintiff has not set forth any qualifying countervailing public interest that would be served by such a disclosure. The release of the withheld identifying information also would not serve the core purpose of FOIA—informing the public as to the operations or activities of the government. Because there is no qualifying public interest in disclosure, CIA determined that the release of this information would constitute a clearly unwarranted invasion of the personal privacy of these individuals. In addition, to the extent the identifying information is that of Agency personnel, the protections of Exemption 3 also apply in conjunction with the CIA Act. [Blaine Declaration, ¶61].

Exemption 7

The OIG is charged with providing objective and independent oversight into the programs and operations of the CIA. On November 13, 2012, the OIG opened an investigation into activities involving former CIA Director Petraeus. After the FBI took over the investigation, the OIG then continued to provide assistance in the investigation. The CIA has asserted Exemptions 7(C) and 7(D) to protect the privacy of those involved in the investigation and information provided by confidential sources to the OIG during the course of its investigation. [Blaine Declaration, ¶63].

Exemption (7)(C)

The CIA invoked Exemption 7(C) here to withhold identifying information regarding the individuals involved in the investigation. The Agency also asserted Exemption 6 for the same personally-identifying information. As with Exemption 6, the Agency withheld the names of CIA employees and other federal government personnel pursuant to Exemption 7(C) because these persons maintain a strong privacy interest. Release of identifying details in connection with this matter could subject them to harassment, embarrassment, or unwanted contact by media or other interested parties, and I am unable to identify any countervailing public interest in revealing the names of these individuals. Accordingly, I have determined that disclosure of this information could reasonably be expected to constitute an unwarranted invasion of personal privacy pursuant to Exemption (b)(7)(C). [Blaine Declaration, ¶64].

Exemption 7(D)

As a matter of Agency policy, the OIG does not disclose the identities of persons it interviews or the substance of their statements unless such disclosure is determined to be necessary for the full reporting of a matter or the fulfillment of other OIG or Agency responsibilities. Pursuant to Agency policy, all interviewees here were under an express or implied promise of confidentiality. The OIG shared this information to the extent necessary for law enforcement purposes. The CIA has asserted Exemption 7(D) to protect the interview notes of OIG investigators and memoranda drafted from those notes. The notes contain details that would tend to identify the individuals interviewed by revealing their position in the Agency or their role in, or knowledge of, the underlying events. The performance of the OIG's mission to conduct independent investigations is heavily reliant upon its access to unfiltered information provided by confidential sources. Disclosure of the sources and the information that they provide would severely compromise the OIG's ability to perform those duties. Because this investigation was criminal in nature, all information provided by these confidential sources is protected by Exemption 7(D). As such, no part of the interview notes or the memoranda is segregable. [Blaine Declaration, ¶65].

Exemption 7(E)

The OIG relies upon certain investigative techniques in order to fulfill its mission of providing objective and independent oversight into the programs and operations of the CIA. The Agency invoked Exemption 7(E) in this case to protect information related to

some of the techniques and procedures used by the OIG in relation to the OIG's investigation into former CIA Director Petraeus. If disclosed, this information would reveal the extent to which the OIG records, catalogs, or otherwise compiles specific information as part of its investigations. This information, if made available, could be used to try to circumvent those techniques and procedures, or neutralize their effectiveness, in association with attempts by others to evade detection in the future. For the limited amount of information for which the CIA asserted Exemption 7(E), the CIA also asserted Exemption 3 under the National Security Act. The techniques and procedures employed by the OIG to conduct its investigations also constitute intelligence methods protected from disclosure under the National Security Act. [Blaine Declaration, ¶66].

F. EXPLANATION OF WITHHOLDING BY ODNI

Plaintiff's June 11, 2020, request to ODNI sought records related to the DNC Hack. [ECF No. 5, Exhibit 5]. In response, ODNI withheld nineteen documents in full, withheld four documents in part, and referred three documents to other agencies. [Koch Declaration, ¶15, Exhibit C]. ODNI withhold information pursuant to FOIA Exemptions 1, 3, 5, 6, 7(A), 7(C), 7(D), and 7(E). ODNI's *Vaughn* index is attached to the Koch Declaration as Exhibit D.

Exemption 1

ODNI determined that each invocation of Exemption 1 in the redacted and withheld documents is proper and consistent with E.O. 13526. ODNI has determined that

the information withheld under Exemption 1 that is responsive to Plaintiff's request is currently and properly classified. Additionally, this information is owned by and is under the control of the U.S. Government. Furthermore, the information withheld under Exemption 1 falls under several classification categories listed within E.O. 13526—namely, "(a) military plans, weapons systems, or operations; (b) foreign government information; (c) intelligence activities (including covert action), intelligence sources or methods, or cryptology; [or] (d) foreign relations or foreign activities of the United States, including confidential sources…." E.O. 13526 § 1.4. Finally, ODNI has determined that unauthorized disclosure of the information withheld under Exemption 1 could reasonably be expected to result in at least serious damage to the national security. This information was therefore properly withheld under FOIA Exemption 1. [Koch Declaration, ¶19-22].

None of the information withheld under Exemption 1 has been classified in order to conceal violations of law, inefficiency or administrative error; prevent embarrassment to a person, organization or agency; restrain competition; or prevent or delay the release of information that does not require protection in the interests of national security. Further, the responsive information is properly marked in accordance with § 1.6 of E.O. 13526. [Koch Declaration, ¶23].

Exemption 3

FOIA Exemption 3 protects information that is specifically exempted from disclosure by statute, if that statute "requires that the matters be withheld from the public

in such a manner as to leave no discretion on the issue" or "establishes particular criteria for withholding or refers to particular types of matters to be withheld." 5 U.S.C. § 552(b)(3). ODNI has determined that three different statutory provisions form a proper basis in this case to withhold information under FOIA Exemption 3.

ODNI has determined that each invocation of Exemption 3 in the withheld and redacted documents is proper and consistent with the "intelligence sources and methods" provision of the National Security Act (50 U.S.C. § 3024(i)(1)) the "personnel" provision of the National Security Act (50 U.S.C. § 3024(m)), 10 U.S.C § 130c, or some combination thereof. The information behind the "(b)(3)" redactions in this case was therefore properly withheld under FOIA Exemption 3. [Koch Declaration, ¶24-28].

Exemption 5

ODNI has determined that each invocation of Exemption 5 is proper and consistent with the deliberative process privilege because the information at issue is both pre-decisional and deliberative. Such information was therefore properly withheld under Exemption 5. [Koch Declaration, ¶29-30].

Exemption 6

ODNI has determined that each invocation of Exemption 6 is proper because: (1) it protects a personnel, medical, or "similar" file or piece of information; (2) there is a significant privacy interest in the underlying information; and (3) such privacy interest outweighs the requester's asserted public interest in the information. Such information was therefore properly withheld under Exemption 6. [Koch Declaration, ¶31-32].

Exemption 7

Exemption 7 generally protects various categories of "records or information compiled for law enforcement purposes." 5 U.S.C. § 552(b)(7). While ODNI is not a law enforcement agency, it may receive, assess, and use intelligence or other information from government agencies that have a law enforcement mission. In such situations, as in this case, ODNI consults with the originating agency or agencies to determine if FOIA Exemption 7 applies to their information. [Koch Declaration, ¶33].

As a result of that consultation process, the Federal Bureau of Investigation ("FBI") requested ODNI to invoke Exemptions 7(A), 7(C), 7(D), and 7(E) over certain information contained within ODNI records that are responsive to the Plaintiff's Request. Respectively, these exemptions apply when the release of law enforcement records "could reasonably be expected to": "interfere with enforcement proceedings;" "constitute an unwarranted invasion of personal privacy;" "disclose the identity of a confidential source;" and disclose investigative techniques and procedures. 5 U.S.C. § 552(b)(7)(A), (C), (D), (E). [Koch Declaration, ¶34].

ODNI has determined that each invocation of Exemption 7 requested by the FBI is proper because the underlying information is subject to one or more of the exemptions contained in Exemptions 7(A), 7(C), 7(D), or 7(E). Such information was thus properly withheld under Exemption 7.

CONCLUSION

The Non-FBI Defendants performed adequate and reasonable searches for responsive records, processed all such records, and released all reasonably segregable non-exempt information from documents responsive to Plaintiff's FOIA requests that are subject to the FOIA. Defendants processed the records under the access provisions of the FOIA to achieve maximum disclosure. Information was properly withheld pursuant to FOIA Exemptions 1, 3, 5, 6, 7(A), 7(C), 7(D), and 7(E), 5 U.S.C. §§552 (b)(1), (b)(3), (b)(5), (b)(6), (b)(7)(A), (b)(7)(C), (b)(7)(D), and (b)(7)(E). The Non-FBI Defendants carefully examined the documents and determined the information withheld from Plaintiff in this case, if disclosed would reveal classified information; would reveal statutorily protected information; would reveal privileged information; could reasonably be expected to interfere with pending or prospective enforcement proceedings; would cause a clearly unwarranted invasion of the personal privacy, or could reasonably be expected to constitute an unwarranted invasion of personal privacy; could reasonably be expected to disclose the identities of confidential sources and the information they provided; and would disclose techniques and procedures for law enforcement investigations. After extensive review of the documents at issue, the non-FBI Defendants have determined that there is no further non-exempt information that can be reasonably segregated and released without revealing exempt information. [Blaine Declaration, ¶67; Cain Declaration, ¶29; Kiyosaki Declaration, ¶23; Koch Declaration, ¶¶36-38].

Because the Non-FBI Defendants conducted reasonable searches in response to Plaintiff's FOIA requests, properly issued *Glomar* responses as appropriate, and properly withheld information pursuant to appropriate FOIA exemptions, the Non-FBI Defendants are entitled to summary judgment.

Respectfully submitted,

BRIT FEATHERSTON
UNITED STATES ATTORNEY

/s Andrea L. Parker
ANDREA L. PARKER
Assistant United States Attorney
Texas Bar No. 00790851
550 Fannin, Suite 1250
Beaumont, Texas 77701
Tel: (409) 839-2538
Fax: (409) 839-2550
Email: andrea.parker@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on February 22, 2022, a true and correct copy of the foregoing document was filed electronically with the court and has been sent to counsel of record via the court's electronic filing system.

/s/ Andrea L. Parker
ANDREA L. PARKER
Assistant United States Attorney